Hewlett Packard
Enterprise

HPE Morpheus VM Essentials Software Documentation

Published: September 2025

HPE Morpheus VM Essentials Software Documentation

Abstract

User Manual for HPE Morpheus VM Essentials Software version v8.0.10

Published: September 2025

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Optane™, Pentium®, Xeon®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the U.S. and other countries.

AMD and the AMD EPYC™ and combinations thereof are trademarks of Advanced Micro Devices, Inc.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

All third-party marks are property of their respective owners.

Table of contents

- HPE Morpheus VM Essentials Software
  - Getting Started
    - Network Considerations
    - Installation
    - Initial VM Essentials manager Setup
    - Upgrading the Manager
      - Setup from the HVM host
      - Setup from another computer
      - Upgrading
    - Compatibility Matrix for HPE Morpheus VM Essentials Software
    - Elevating to HPE Morpheus Enterprise
  - Operations
    - Dashboard
      - Environment
      - System Status
      - Favorites
      - Instance Status
      - Instances By Cloud
      - Group Workloads
      - Cloud Workloads
      - Cluster Workloads
      - Backups
      - Task Executions
      - Activity
    - Wiki
      - Highlights
      - Creating Wikis
      - Hosting Images
    - Activity
      - Activity
        - To View a Recent Activity report:
        - Review
      - History
  - Provisioning
    - Requirements
      - VM Provision Steps
      - Virtual Images
        - Synced Images
        - Local Virtual Images

- Agent Install
  - Agent Install Modes
    - For All Agent Install modes
  - SSH/Winrm
    - Linux Agent
    - Windows Agent
  - VMware tools (vmtools) RPC mode
  - Cloud-Init Agent install mode
- Provisioning Concepts
  - Instances
  - Containers / Nodes / Virtual Machines
  - Hosts / Servers
- Instances
  - Creating Instances
    - Converting Discovered Resources to Managed Instances
  - Managing Instances
    - Actions
    - Performing Instance Actions
    - Notes

- Library
  - Labels
    - Adding and Removing Labels
    - Running Automation Against Label Targets
  - Automation
    - Tasks
      - Role Permissions
        - Common Options
      - Target Options
      - Execute Options
      - Source Options
      - Allow Custom Config
        - Example JSON Map:
        - Task Types
        - Task Management
      - Adding Tasks
      - Editing Tasks
      - Deleting Tasks
    - Execute Scheduling
  - Virtual Images
    - Overview
    - Configuring Virtual Images

        - User Images
            - To edit and configure an existing Virtual Image:
    - Provisioning Images
    - Add Virtual Image
        - VMware - VM Templates Copies
- Infrastructure
    - Groups
        - Overview
        - UI
        - CLI
        - API
        - Adding Groups
        - Managing Groups
        - Edit Group
        - Delete Group
        - User Access
    - Clouds
        - Overview
        - Creating Clouds
        - Cloud Detail View
            - Cloud Detail Tabs
        - Deleting Clouds
    - Clusters
        - Overview
        - Requirements
        - Cluster Permissions
        - HVM clusters
            - Features
                - Host Features
                - VM Features
            - Base Cluster Details
                - Hardware Requirements
                - Example Cluster Deployment
            - Provisioning the Cluster
            - HVM Cluster Networking
            - Provisioning a Workload
            - Monitoring the Cluster
                - Moving Workloads Between Hosts
                - Adding hosts
                - Maintenance Mode
                - Affinity Groups

        - Failover
        - Adding an NFS Datastore
    - Image Prep (Windows)
    - Utilizing Existing QCOW Images from an NFS File Share
    - Hardware Passthrough
        - Creating Service Plans
        - Viewing and Assigning Hardware Devices
        - GPU Passthrough Example
- Network
    - Networks
        - Overview
        - Configuring Networks
            - DHCP
            - Static and IP Pools
            - Advanced Options (Search Domains)
            - Group and Tenant Access
            - Guest Console SSH Tunnel
            - Subnets
    - Network Groups
        - Adding Network Groups
    - Routers
        - Overview
        - Create New Router
        - Editing Existing Routers
        - Deleting Existing Routers
    - IP Pools
        - Overview
        - To add a VM Essentials Network Pool
    - Floating IPs
        - Overview
        - Floating IPs List Page
        - Working with Floating IPs
    - Domains
        - Overview
        - Adding Domains
        - Editing Domain Permissions
            - Group Access
        - Editing and Removing Domains
        - Setting the default domain on a Cloud
        - Setting the default domain on a Network
        - Selecting a Domain while provisioning an Instance

- Proxies
  - Overview
  - Defining Proxies
  - Cloud Communication
  - Provisioning with Proxies
- Integrations
  - Overview
  - Scoping Services

- Storage
  - Role Requirements
  - Default Storage
    - Storage Buckets
  - Supported Bucket Types
  - Alibaba Buckets
  - Amazon S3 Buckets
  - Azure Buckets
  - Google Cloud Storage Buckets
  - Dell EMC ECS Buckets
  - Openstack Swift Buckets
  - Rackspace CDN Buckets
    - File Shares
  - Supported File Share Types
  - CIFS File Shares
  - Local Storage File Shares
  - NFSv3 File Shares
    - Data Stores
  - Create Data Stores
  - Manage Permissions
    - Servers
  - Add Storage Server
- Trust
  - Credentials
  - OAuth 2.0 Credentials
    - Add Existing Key Pair
    - Generate Key Pair
    - Delete Key Pair
  - Key Pairs
    - Add Existing Key Pair
    - Generate Key Pair
    - Delete Key Pair

- Backups

        - Initial Backups Setup
            - Global Backups Settings
            - Execution Schedules
        - Configuring Backups during Provisioning
        - Summary
        - Backups
            - Create an Instance Backup
    - Tools
        - Cypher
            - Overview
            - Mountpoints
            - Creating Cypher Keys
            - Password
            - tfvars
            - Secret
            - UUID
            - Key
            - Vault
            - Editing Cypher Keys
            - Using Cypher Keys in Scripts
        - Archives
            - Overview
            - Archives List Page
            - Adding an Archive
            - Archive Detail Page
            - File Detail Page
        - Migrations
            - Overview
            - Migrations Requirements
            - Migrations Plans
            - Configuring Windows Workloads (Windows 2022 or later) for Migration
            - Migrating a Windows VM (Online procedure)
    - Administration
        - Identity Sources
            - Overview
        - Plans & Pricing
            - Overview
                - Create Service Plan
                - Service Plan Permissions
                - Service Plan Configuration
        - Roles

- Overview
  - Role Creation
- Roles and Identity Sources
- Role Permissions
  - Role Permission Sections
  - Feature Access Permissions

- Users
  - Users
    - Overview
    - Create User
    - Edit User
    - User Settings

- Health
  - VM Essentials Health
    - Health Levels
    - Additional System Health Indices
  - Logs

- Settings
  - Appliance
    - Appliance Settings
    - Tenant Management Settings
    - User Management Settings
    - Email Settings
    - Twilio SMS Settings
    - Proxy Settings
    - Currency Settings
    - Integrating With a Currency Exchange Provider
    - Consuming Currency Exchange in VM Essentials
    - Enabled Clouds (Types)
  - Provisioning
    - Provisioning Settings
    - Cloud-Init Settings
    - Windows Settings
    - Library Settings
    - PXE Boot Settings
    - App Blueprint Settings
    - Terraform Settings
  - Backups
    - Backup Settings
      - VM Essentials Backup Settings
  - Environments

        - Overview
            - Creating Environments
    - License
        - Overview
        - Current License
        - Upgrade License Key
    - Utilities
- User Settings
    - User Photo
    - User Settings
    - 2 Factor Authentication
        - Setting Up Two-Factor Authentication
        - Disabling Two-Factor Authentication
        - Handling User Lock-Out
    - Preferences
    - Linux Settings
    - Windows Settings
    - API Access
- Guides
    - Integration Guides
        - Clouds
            - VMware vCenter
                - Overview
                - Features
                - Getting Started
                - Windows Provisioning Tips
                - Existing Instances
                - Service Plans
                - Virtual Images / Blueprints
                - Snapshots
                - Affinity Groups
                - Tagging and Metadata
                - Advanced
                - VMware Permissions
                    - Create vCenter Users and Roles
                    - Privileges
                    - Usage
                - Creating a VM Essentials VMware Image
                - Creating a CentOS/RHEL 7 Image
                    - Cloud-Init
                    - Network Interfaces

        - Creating a CentOS/RHEL 8 Image
            - Prepare The New CentOS 8/RHEL8 Image
            - SELinux Settings
            - Network Interfaces
            - Final VMWare Tasks
            - Creating an Ubuntu 20.04 Image
        - Gotchas
        - A Note on Proxies
- Networking Integrations
    - ArubaCX Network Integration
        - Overview
        - Features
        - Prerequisites
            - Server Network Configuration (Netplan)
            - Switch Configuration
        - Adding ArubaCX Integration
        - Add ArubaCX Integration to a Cluster
    - HPE Aruba CX DSS
        - Overview
        - Features
        - Prerequisites
        - Adding HPE Aruba CX DSS Network Integration
        - Create HPE ANW DSS Port Group Network
        - Delete HPE ANW DSS Port Group Network
        - View HPE Aruba CX DSS Network Integration
- Storage
    - HPE Alletra MP Storage
        - Prerequisites
        - Add HPE Alletra MP Storage
        - Create Datastore
        - Create Instance
        - Add a storage server
            - Viewing the Summary page
            - Viewing Alerts
            - Viewing Volumes
- Image preparation
    - Image Prep (Windows)
    - Creating a Windows Image
        - Supported Versions
        - Image Preparation
    - Creating a VM Essentials VMware Image

- Creating a CentOS/RHEL 7 Image
  - Cloud-Init
  - Network Interfaces
- Creating a CentOS/RHEL 8 Image
  - Prepare The New CentOS 8/RHEL8 Image
  - SELinux Settings
  - Network Interfaces
  - Final VMWare Tasks
  - Creating an Ubuntu 20.04 Image

HPE Morpheus VM Essentials Software

Subtopics

- Getting Started
- Operations
- Provisioning
- Library
- Infrastructure
- Backups
- Tools
- Administration

Getting Started

HPE Morpheus VM Essentials Software is a unified solution allowing for easy deployment of KVM-based HVM workloads and intuitive integration of existing VMware vCenter Clouds, all with administration made easy through the HPE Morpheus VM Essentials Manager. Once deployed, take advantage of powerful features including live migration of VMs across HVM Cluster hosts with zero downtime, dynamically distribute workloads based on load, automatic failover of workloads following the loss of a host, and a lot more. Provisioning new workloads is also made easy with the VM Essentials image library, automation tools, and powerful provisioning wizard. In addition to HVM clusters, VM Essentials also includes a deep integration into VMware vCenter, which also takes advantage of the same powerful provisioning wizard, automation engine, and monitoring capabilities.

This documentation covers the system requirements for HVM clusters and a setup guide for installing VM Essentials manager. It also includes example use cases for effective implementation of the feature set and in-depth sections for each area of the UI detailing the capabilities of each tool.

Before getting started, it's important to note that administrators have the responsibility to install and configure servers and network equipment in a way that will ensure successful operation of VM Essentials. This includes selecting host servers, storage hardware, and networking hardware that have been certified as compatible with the platform. The VM Essentials section of the **HPE Support Center** contains a reference architecture document which includes a validated design with specific hardware SKUs. The same section of the HPE Support Center also includes a qualification matrix which lists hardware that has been certified compatible.

Additionally, administrators will be required to perform some setup functions on their own, such as preinstalling Ubuntu 24.04 (or 22.04 though you won't be able to utilize the latest cluster layouts) on host servers, configuring networking for each host, configuring access to external storage at the OS level, and establishing a network topology that ensures acceptable performance. Subsequent sections of this document will outline some effective network designs and some tips for selecting a network design based on available hardware. It will be the responsibility of the administrator to select a network design based on available hardware and to use the Linux command line to establish appropriate network bonds, storage configuration, and access across the cluster.

Subtopics

- Network Considerations
- Installation
- Initial VM Essentials manager Setup
- Upgrading the Manager
- Compatibility Matrix for HPE Morpheus VM Essentials Software
- Elevating to HPE Morpheus Enterprise

Network Considerations

In order to run VM Essentials effectively in production, network redundancy and throughput must be considered. Network bonding is an important component to building redundancy into the environment so we will briefly discuss it here before showing some example network configurations. Ultimately the environment is your own but this discussion and the example network configurations that follow will help in planning out an effective operating environment for VM Essentials.

NOTE

In the Ubuntu installer, if you configure the IPv4 network, save, and then return to edit it, the gateway and DNS server configurations are no longer present. However, if you continue on with the installation, the configured information does end up in the netplan. This is a known issue with the Ubuntu installer.

Network Bonding

Network bonding is the combining of multiple network adapters into a single logical interface. This is done to build in redundancy and to increase throughput. Network bonds are configured at the operating system level and there are multiple types of network bonds depending on hardware support and other factors.

In the scenarios described in the following sections, we will call out two types of network bonds that are effective for virtualization (active-backup and LACP) and show them in example configurations. VMware LBT bonds are also shown in the table below for the sake of comparison, though only the other two have been utilized in verified scenarios.

Once established, we can later offer up these bonded interfaces as a compute network (for virtual machine traffic) or storage network (for interacting with external storage) when creating our cluster within the VM Essentials manager.

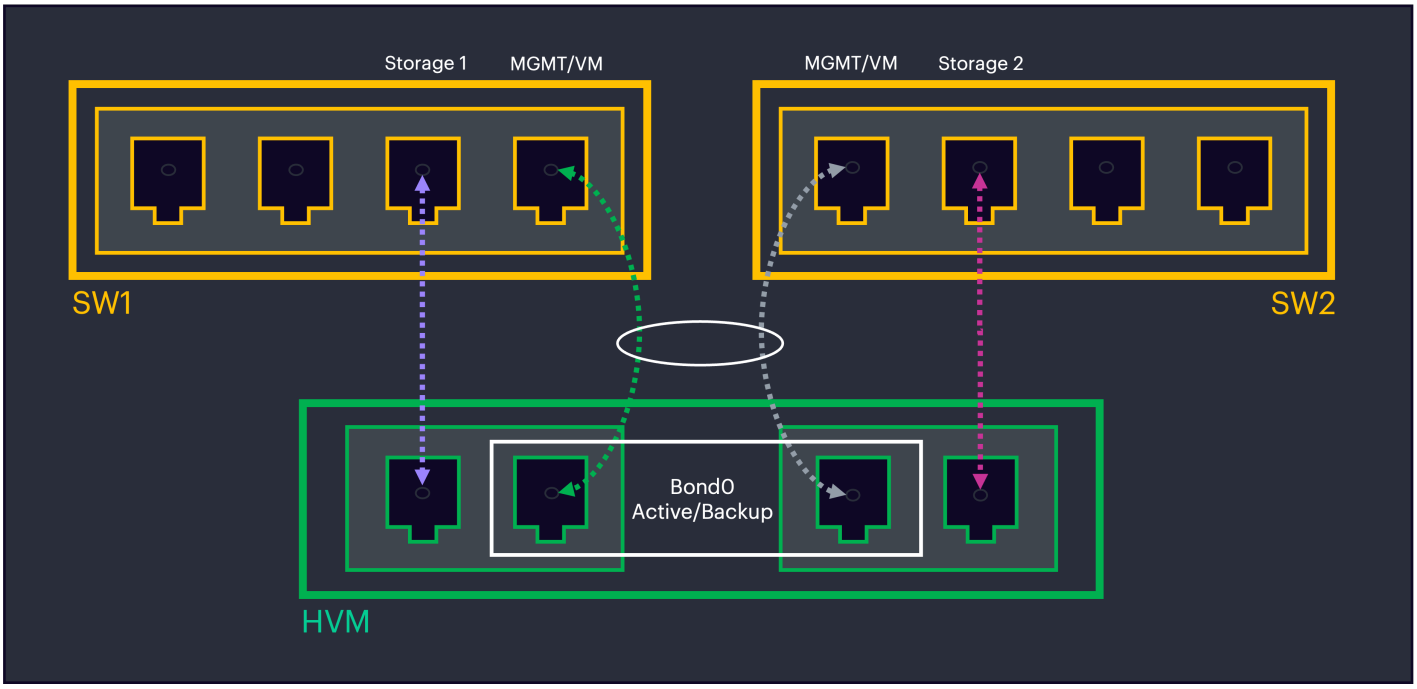
Feature	VMware LBT	Active-backup	802.3ad (LACP)
Switch config required	❌	❌	✅ Yes (LACP Support)
Outbound load balancing	✅ (NIC load based)	❌	✅ (Outbound + Inbound)
Inbound Failover	❌ (Depends on switch)	✅ (Instant failover)	✅ (Switch handles failover)
NIC Utilization	Dynamic	One Active NIC	Full duplex load balancing
Failover Speed	Fast (Outbound only)	Very Fast (link state)	Fast (Switch + Driver)
Complexity	Low	Very low	High (Switch + Host Config)
Best for	Balanced outbound traffic	Simplicity + Resilience	High performance switch-aware setups

Example Network Configurations

If you have the capability to do so, it's recommended you set up networking with full redundancy. Such a setup could include two network switches and hosts with at least six network interfaces spread across two network cards. This would allow for failover in the event of the loss of a switch and/or one of the host network cards in addition to separating management and compute network traffic to their own interfaces. Hosts with only four NICs each can still be configured for full redundancy but would have to converge management and compute traffic across the same interfaces. Keep in mind also that these examples use MPIO (multi-path input/output) for storage. It would also be possible to use bonding for storage depending on capabilities of the environment. MPIO is recommended whenever fibre channel or iSCSI LUNs are being used for GFS2 datastores.

Scenario 1: Recommended Converged Networking Setup

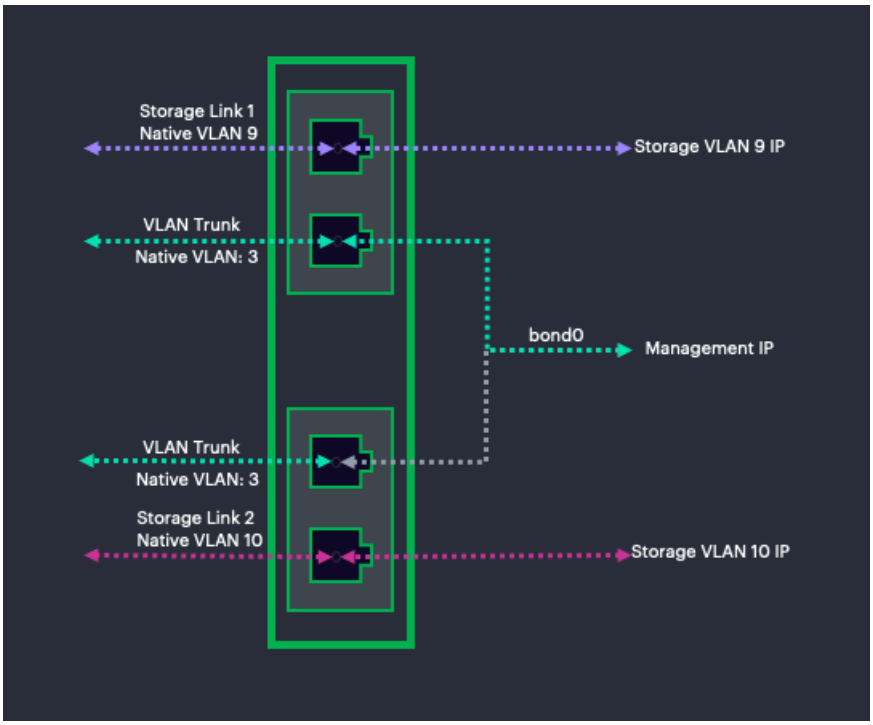
Let's first take a look at two converged networking examples. This is where management and VM traffic is converged over the same bonded interface and storage traffic is independent. In an ideal scenario, you would have at least four network interfaces spread across at least two network cards on the host (shown in green on the diagram below). Ideally you would also have two separate network switches to help ensure resiliency and redundancy. As mentioned in the prior section, these networking examples are all created with resiliency and redundancy in mind. One storage lane is connected to each switch and likewise one management/VM lane is connected to each switch, which are bonded in and active/backup configuration. Consult the bonding table in the prior section for more details on the benefits and drawbacks to different types of network bonds. In this scenario, the bond handles management/VM traffic failover while multipathing handles storage failover. A diagram of such a network setup is shown below:



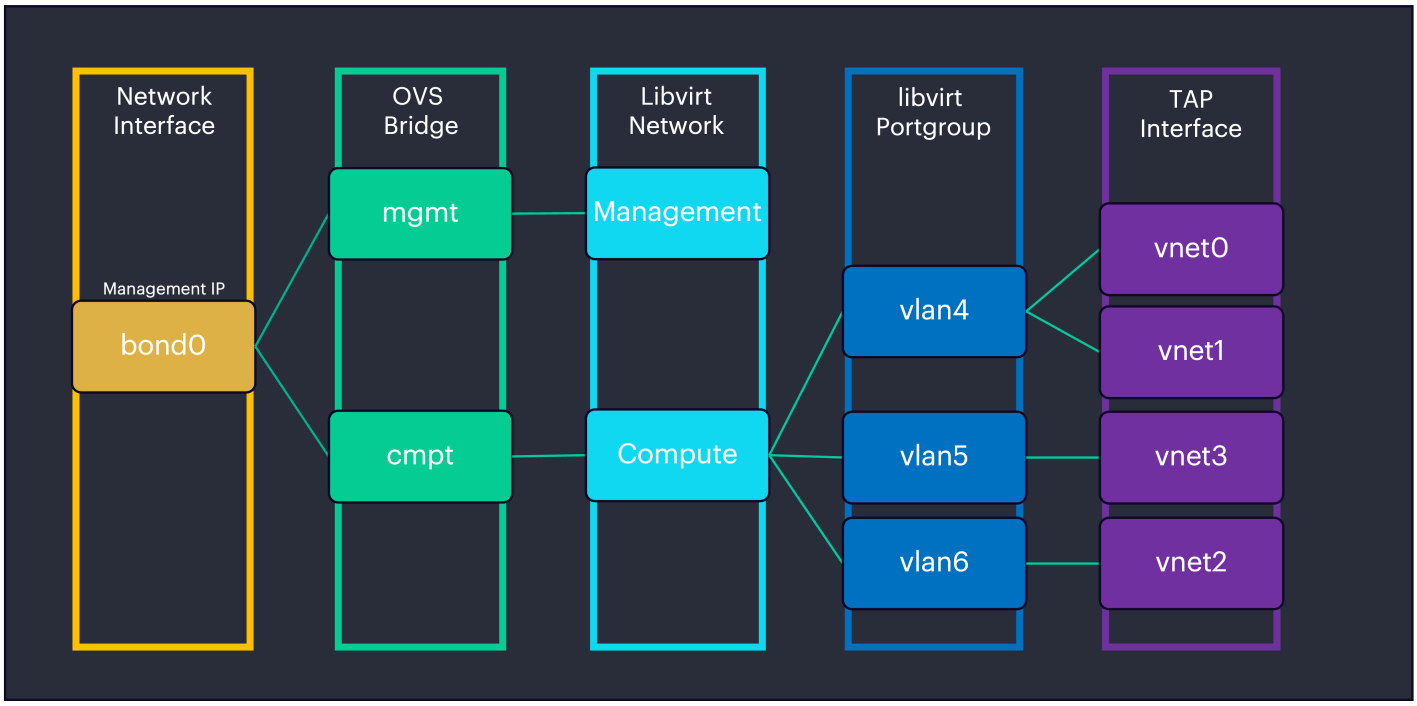
In the example below, we have native VLAN on the trunk ports and on the storage ports. This means the network switch is tagging all the traffic for you and you don't have to tag it yourself. This allows you to put your IP addresses directly on the interfaces and bonds. Here, the storage VLANS get their own IP address directly on the interface while the management IP address goes directly on the bond as shown in the diagram below. With this configuration, all can be done in the installation wizard as long as the VLANs are piped to the interfaces as expected from the network switches. More specific guidance on using the installation wizard is included in later sections covering the software installation.

NOTE

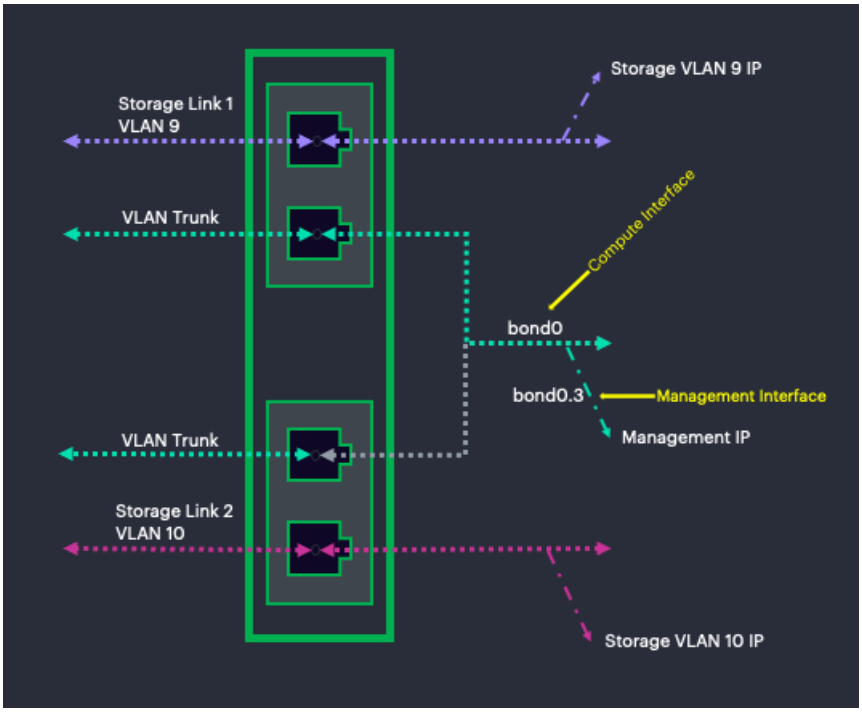
Your environment an configurations will vary. You may or may not have a native VLAN set up for storage traffic as it is best practice to isolate storage traffic when possible. The need for VLAN tagging on specific interfaces is dependent on whether there is a native VLAN on that interface.



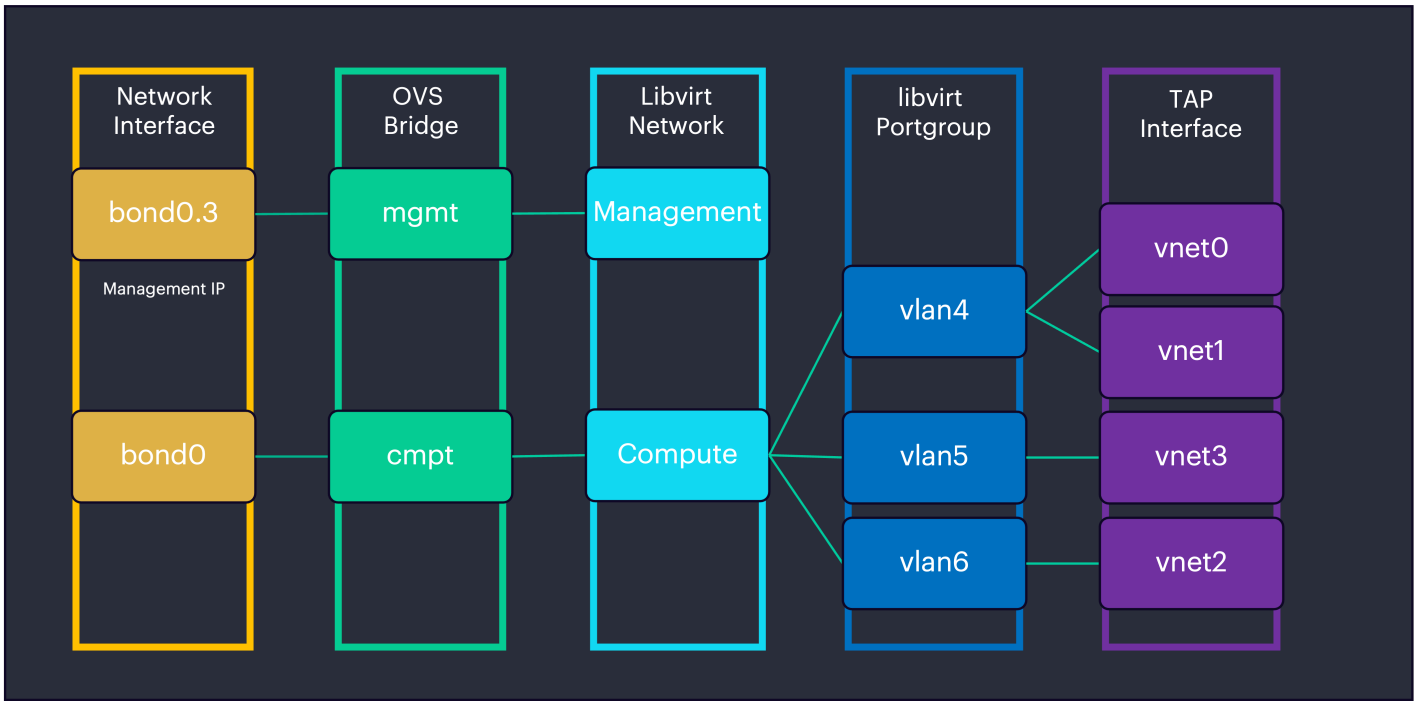
Below is a chart showing the connection from the bonded network interfaces created in the example network configuration above to OVS bridges (a virtual switch that connects VMs to the physical network), Libvirt Networks (logical virtual networks managed by Libvirt), Libvirt Portgroups (subgroups within Libvirt Networks that can expose configurations, such as VLAN tagging), and tap interfaces (the virtual connection that connects the VM to the OVS bridge).



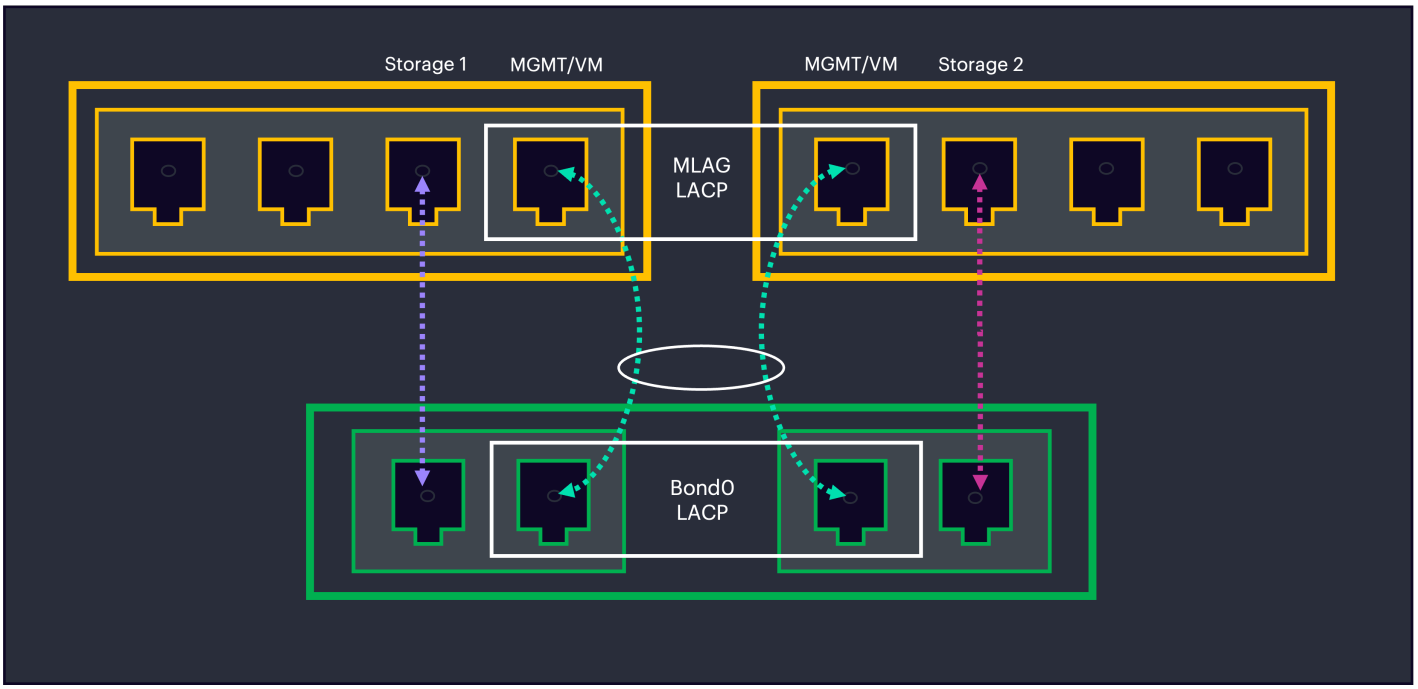
The prior example included native VLANs on the trunk ports and storage ports so we'll now take a look at an example configuration without native VLANs. You need to create VLAN tags on the interfaces because the switch is no longer handling the tagging for you. Your IP addresses then go on those VLAN tags. In this example bond0 becomes the compute interface and bond0.x becomes the management interface when configuring the cluster in a later step. When not using a native VLAN, the storage VLANs still get their own IP address and interface but a VLAN interface gets created on the bond and the management IP address goes on the VLAN interface.



Just as in the similar chart above, the chart below shows the connection from the bonded network interfaces created in the example network configuration above to OVS bridges (a virtual switch that connects VMs to the physical network), Libvirt Networks (logical virtual networks managed by Libvirt), Libvirt Portgroups (subgroups within Libvirt Networks that can expose configurations, such as VLAN tagging), and tap interfaces (the virtual connection that connects the VM to the OVS bridge).

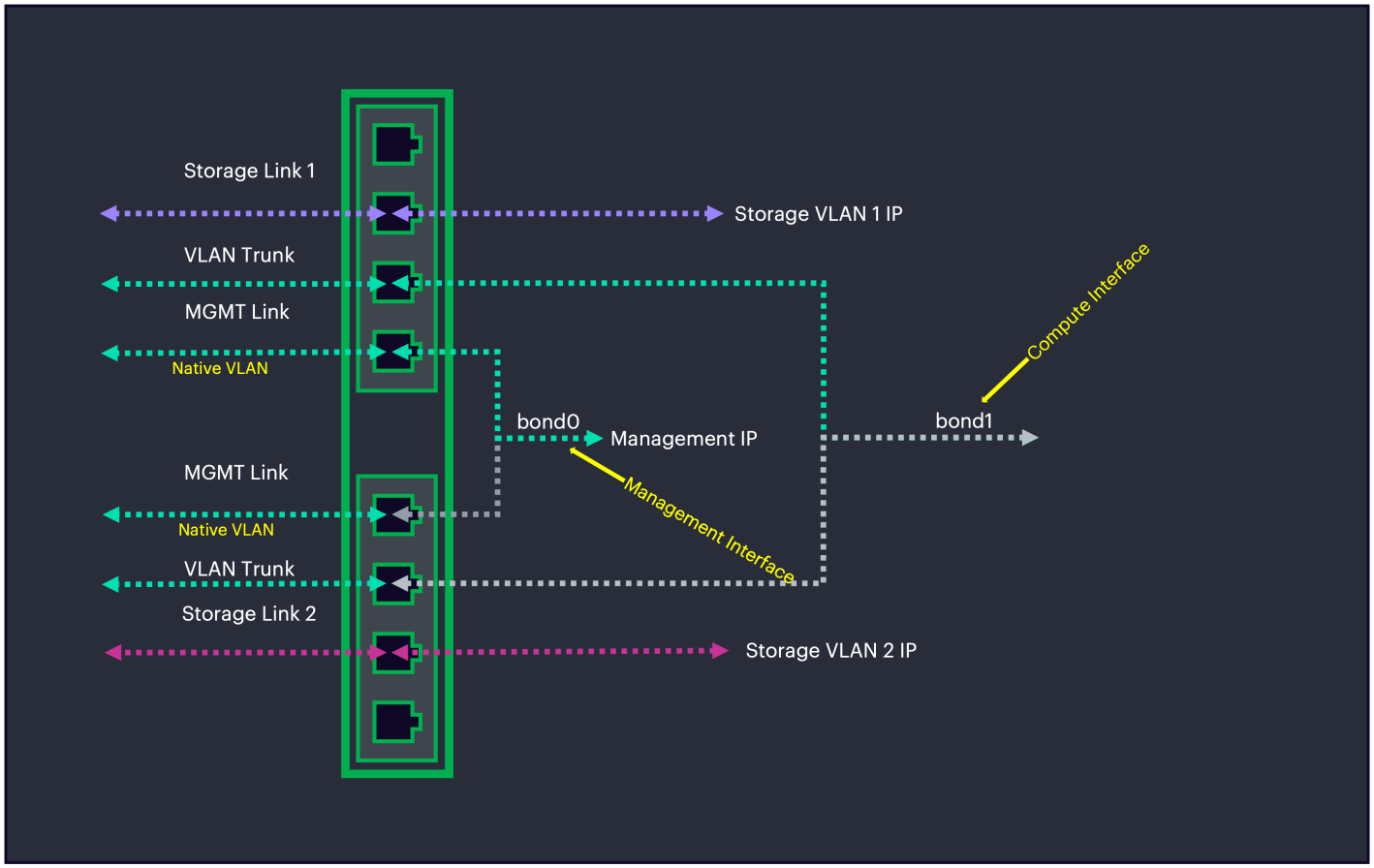


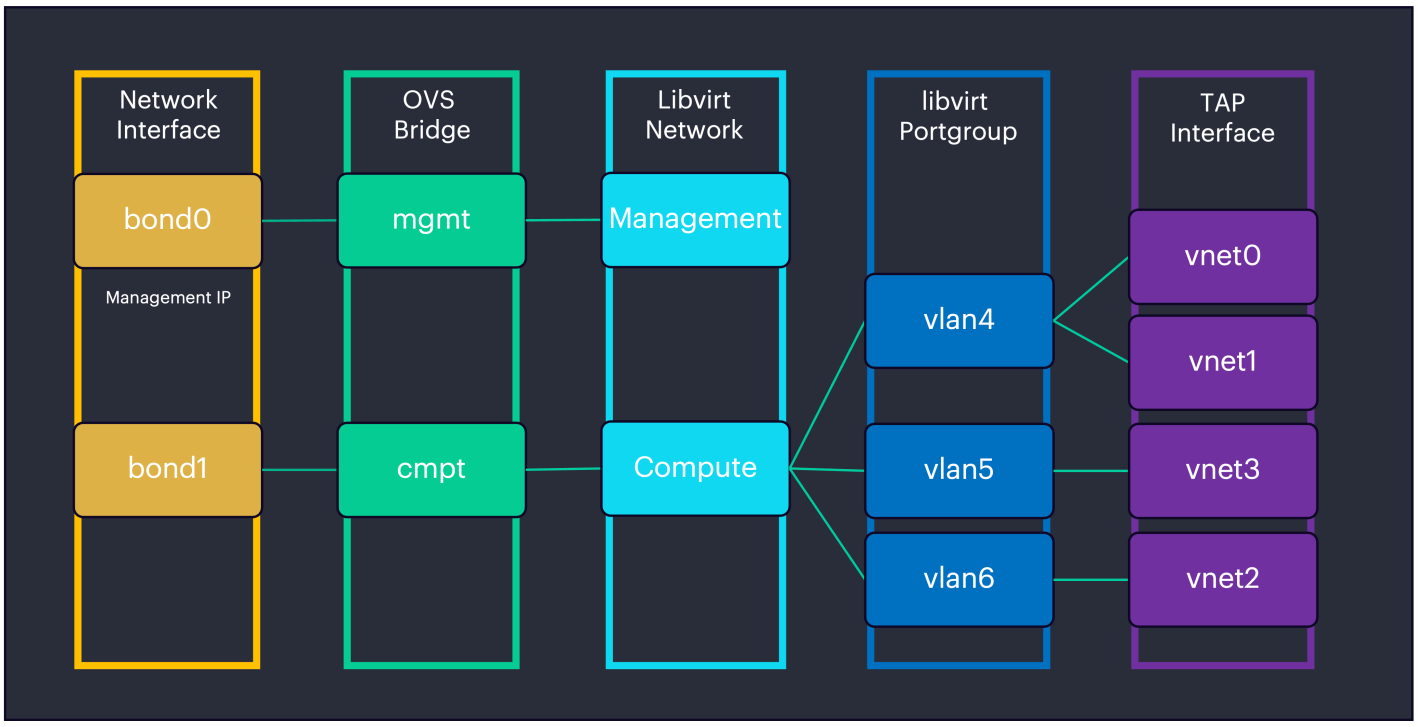
The same networking setup can be used with an LACP bond, however this does require extra configuration on the network switch side. The exact setup steps would depend on the specific hardware in your environment. The network setup would look something like the example below:



Scenario 2: Recommended Decoupled Networking Setup

When hosts have six or more network interfaces spread across at least two cards, management and VM traffic can be separated for even greater network throughput. The overall configuration is very similar. The storage lanes are still separated as they were previously. In this case, create an additional bond across two of the interfaces for VM traffic. As previously, a bond is also created for management traffic. In this example, these bonds are created in an active/passive configuration.





Installation

Having completed a discussion of networking considerations in the previous section, let's now turn to OS installation on the HVM hosts. The hosts are recommended to be HPE Proliant physical servers or other compatible server types (see the **compatibility matrix** for a list of recommended compute server choices) and must be running Ubuntu 24.04 to utilize the latest cluster layout (HVM hosts running Ubuntu

22.04 may also be used but are only compatible with HVM cluster layout version 1.1). For base OS installation on HVM Hosts, Hewlett Packard Enterprise provides an HVM OS Install ISO in My HPE Software Center. This is a pre-patched Ubuntu 24.04 minimal ISO with `kvm` and `hpe-vm` (which is the installation GUI tool) pre-installed.

TIP

Utilizing the HVM OS Install ISO to install the base HVM Host operating system is especially useful for disconnected sites (dark sites) without access to the Internet. This ISO contains Ubuntu 24.04 minimal pre-patched and including required `kvm` and `hpe-vm` packages. When these packages are not present, the installer will attempt to download them from the Internet, which may not be available in all environments. By installing HVM OS, you will only need to provide a few assets from My HPE Software Center to your HVM Hosts and will not need Internet access to pull down other required packages.

The HVM hypervisor runs on top of the Ubuntu hosts. We'll get to the installation portion in the next section but for now we will discuss the system requirements and recommendations for network and storage configuration during the installation.

NOTE

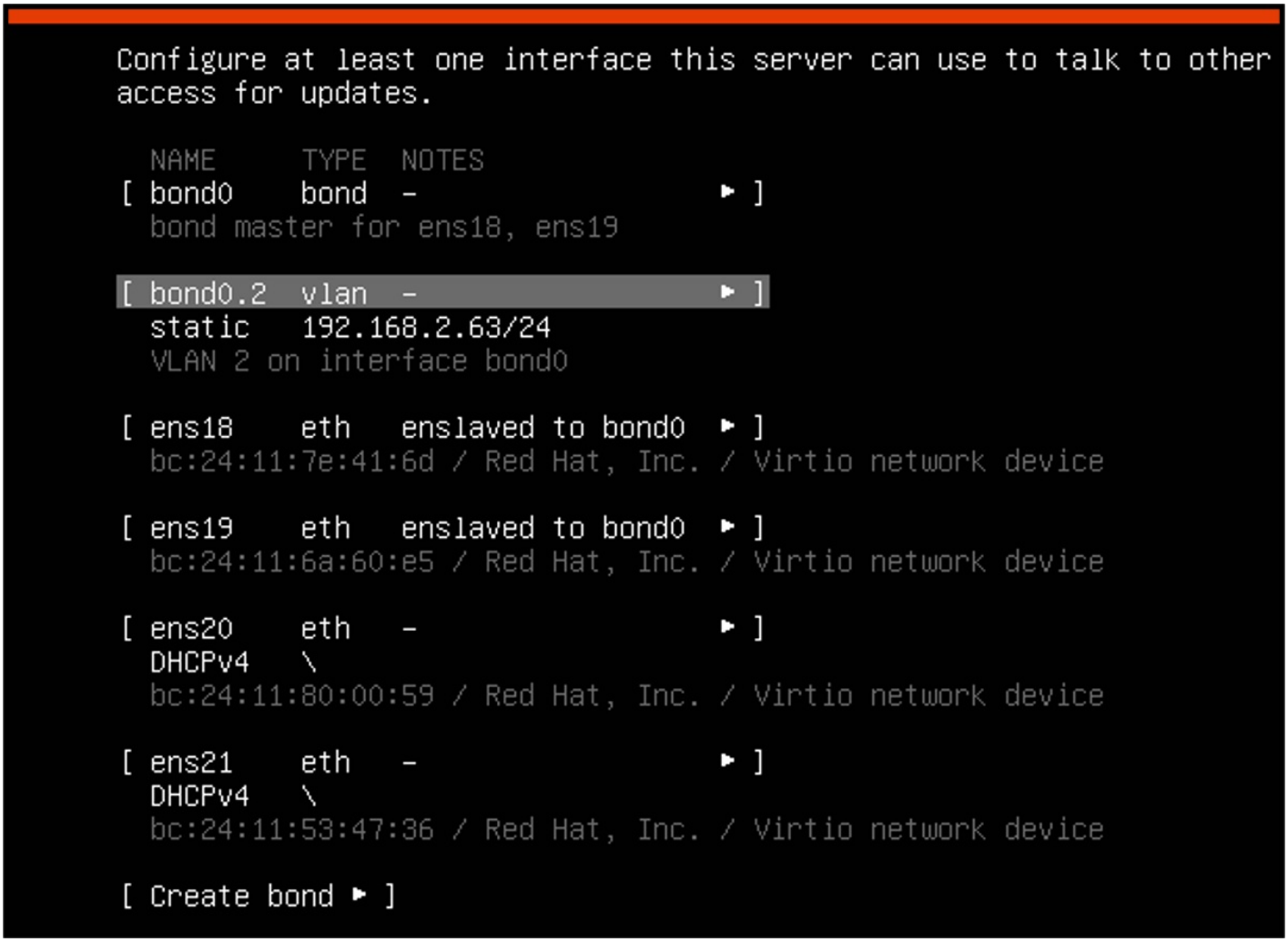
CEPH is not supported in Morpheus 8.0.10 or higher.

Host Requirements

- **Operating System:** Ubuntu 24.04 to utilize the latest HVM cluster layout. Hewlett Packard Enterprise provides a base OS install ISO as a download in My HPE Software Center (HVM OS Install ISO). This is a pre-patched Ubuntu 24.04 minimal ISO with `kvm` and `hpe-vm` (which is the installation GUI tool) pre-installed.
- **Hardware:** HPE Proliant server hardware or another compatible server type is recommended (see the **compatibility matrix** for a list of recommended compute server choices). This list is continually expanded as additional hardware SKUs are tested and verified.
- **CPU:** One or more 64-bit x86 CPUs, 1.5 GHz minimum with Intel VT or AMD-V enabled
- **Memory:** Minimum of 8GB for non-hyperconverged (HCI) deployments or 8GB plus 4GB for each data disk for HCI deployments
- **Storage:** Minimum of 50GB for operating system storage
- **Network:** 100 Mbps or faster NIC (10 Gbps recommended)
- **IP Addressing:** Static IP address
- **Internet Connectivity:** Internet access is required to download and install the required packages and dependencies

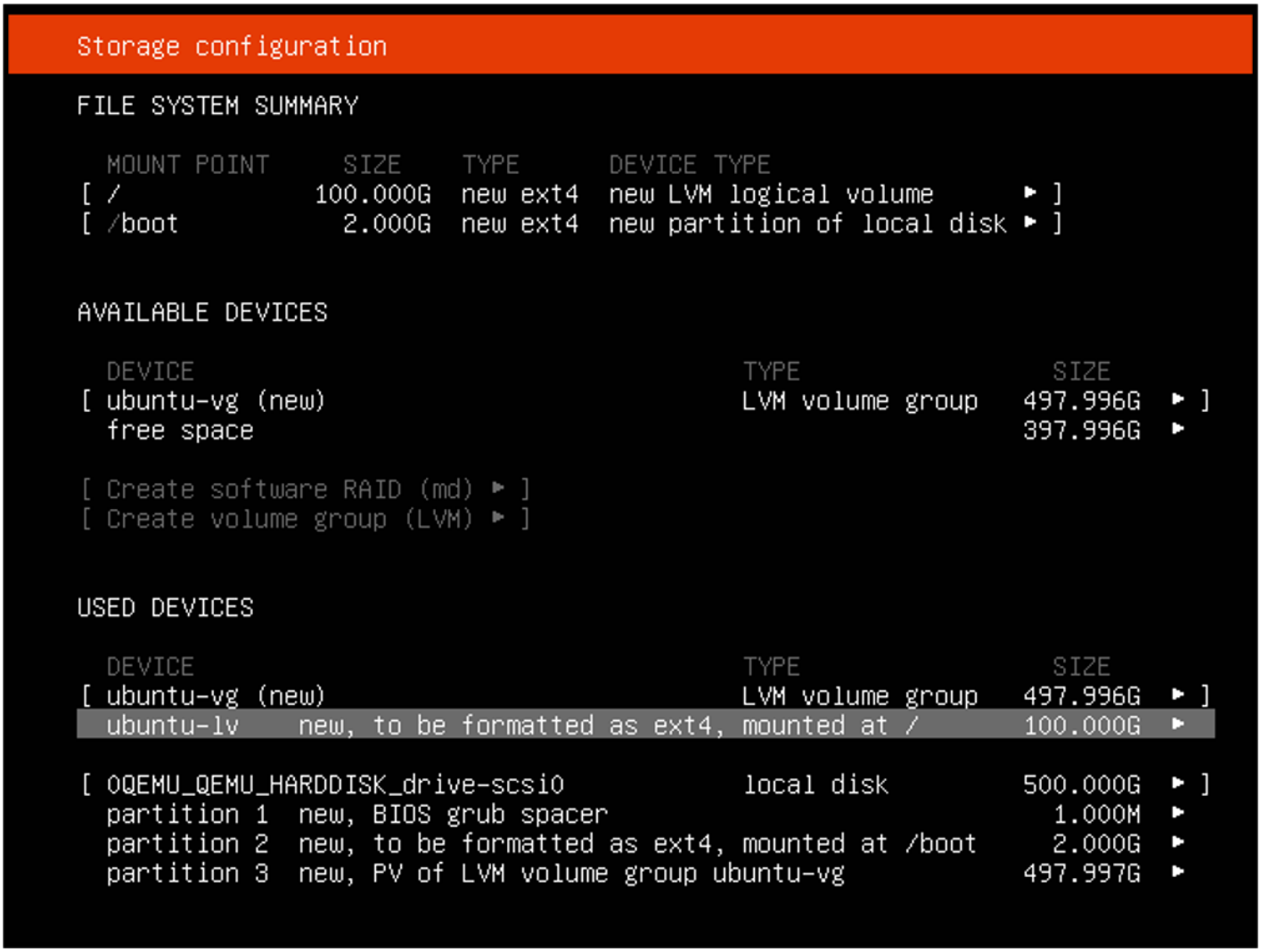
Ubuntu Network Setup

During the networking setup portion of the OS installation, with some network configurations you might have to create the initial bond for the management network in order to get initial connectivity. Bonds can be created from the Ubuntu deployment wizard itself and a discussion of different bond types and their potential usefulness within an effective VM Essentials networking scheme is described in greater detail in the previous section. In the screenshot below, the host is using a converged management and compute interface bond. The bond was created and a VLAN added to the bond. After creating the VLAN, an IP address was assigned at which the individual host can be managed. Thus, when setting up the cluster later, we can identify the `bond0.2` interface for host management traffic and `bond0` as the interface to send all compute traffic. Of course, this is a specific caveat that may not apply such as if you're not using converged networking (described in the previous section) or if DHCP is configured.


Configure at least one interface this server can use to talk to other
access for updates.
NAME TYPE NOTES
[bond0 bond - ▸]
bond master for ens18, ens19
[bond0.2 vlan - ▸]
static 192.168.2.63/24
VLAN 2 on interface bond0
[ens18 eth enslaved to bond0 ▸]
bc:24:11:7e:41:6d / Red Hat, Inc. / Virtio network device
[ens19 eth enslaved to bond0 ▸]
bc:24:11:6a:60:e5 / Red Hat, Inc. / Virtio network device
[ens20 eth - ▸]
DHCPv4 \
bc:24:11:80:00:59 / Red Hat, Inc. / Virtio network device
[ens21 eth - ▸]
DHCPv4 \
bc:24:11:53:47:36 / Red Hat, Inc. / Virtio network device
[Create bond ▸]

Ubuntu Storage Setup

During the storage setup portion of the OS installation, keep in mind that the entire disk won't be utilized by default when using LVM. You'll need to grow the disk. This guide won't discuss that process in complete detail but there are plenty of guides available on the Internet if they are needed.


Storage configuration
FILE SYSTEM SUMMARY
MOUNT POINT SIZE TYPE DEVICE TYPE
[/ 100.000G new ext4 new LVM logical volume ▸]
[/boot 2.000G new ext4 new partition of local disk ▸]
AVAILABLE DEVICES
DEVICE TYPE SIZE
[ubuntu-vg (new) LVM volume group 497.996G ▸]
free space 397.996G ▸
[Create software RAID (md) ▸]
[Create volume group (LVM) ▸]
USED DEVICES
DEVICE TYPE SIZE
[ubuntu-vg (new) LVM volume group 497.996G ▸]
ubuntu-lv new, to be formatted as ext4, mounted at / 100.000G ▸
[QEMU_QEMU_HARDDISK_drive-scsi0 local disk 500.000G ▸]
partition 1 new, BIOS grub spacer 1.000M ▸
partition 2 new, to be formatted as ext4, mounted at /boot 2.000G ▸
partition 3 new, PV of LVM volume group ubuntu-vg 497.997G ▸

External Storage Setup

Though it is possible to utilize local storage on the hosts, more commonly HVM clusters will be configured to interface with external storage. Currently, connecting to external storage over iSCSI and Fibre Channel is supported, see **the compatibility matrix** for a current list of vetted hardware and protocols. External storage provides a number of redundancy capabilities that aren't realized through local storage, such as automatic failover when a host is lost and migrating workloads to new hosts with zero downtime.

Configuring connections to external storage must be done on each host at the OS level. This is part of preparing the hosts for installation of the VM Essentials console and manager. This is done by going to the Ubuntu command line on each host and configuring the initiator to talk to the target. Once this is done and the disk is presented up to the OS, the groundwork is laid for configuring the datastore within VM Essentials manager. This process of creating a new datastore within the Manager UI is shown later in this guide following installation.

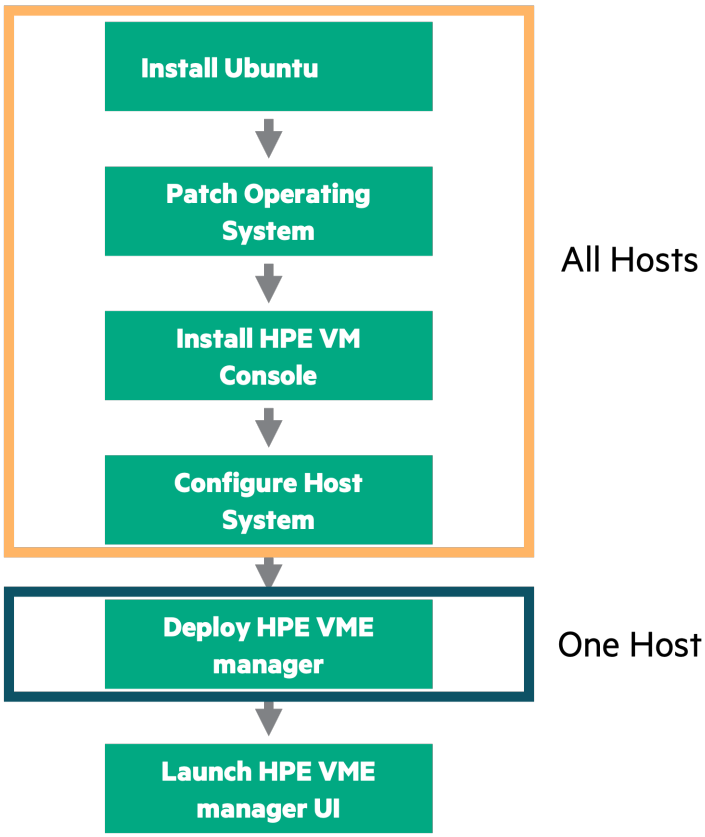
How the storage traffic is routed will depend on networking configuration. Having dedicated storage interfaces, as shown in the network examples from the previous section, is important for optimal throughput and resiliency. After establishing the datastore in the VM Essentials manager UI, this will ensure the operating system is utilizing those dedicated routes rather than through other interfaces that might be available.

Console Installation and Configuration

It's time to begin the actual installation process on the hosts. From a high level, the process is as follows:

- Install using the HVM OS Install ISO (This is recommended over a base Ubuntu 24.04 installation as it comes pre-patched and pre-installed with required `kvm` and `hpe-vm` packages. This is especially ideal for dark sites without Internet access as the required packages are already installed. If a base Ubuntu 24.04 installation is used, the `hpe-vm` installation GUI used to set up the initial cluster will attempt to install the required packages from the Internet). Ubuntu 24.04 is required to use the latest HVM Cluster layouts
- Patch Ubuntu 24.04 with the latest updates and security fixes (especially if using a base Ubuntu 24.04 OS install rather than the provided HVM OS Install ISO)

- Install VM Essentials Console (not required if the HVM Hosts are initially installed from HVM OS Install ISO rather than a vanilla Ubuntu installer). This is a light Debian package that is used to configure the hosts and bootstrap initial virtualization capabilities. This is done on all hosts
- Configure the host system for networking, storage, NTP, etc
- Deploy the VM Essentials manager using the VM Essentials Console. This is done on only one host
- Launch the VM Essentials manager UI and apply license. Note that a short-term evaluation license will automatically be applied for testing purposes if a permanent license is not immediately available

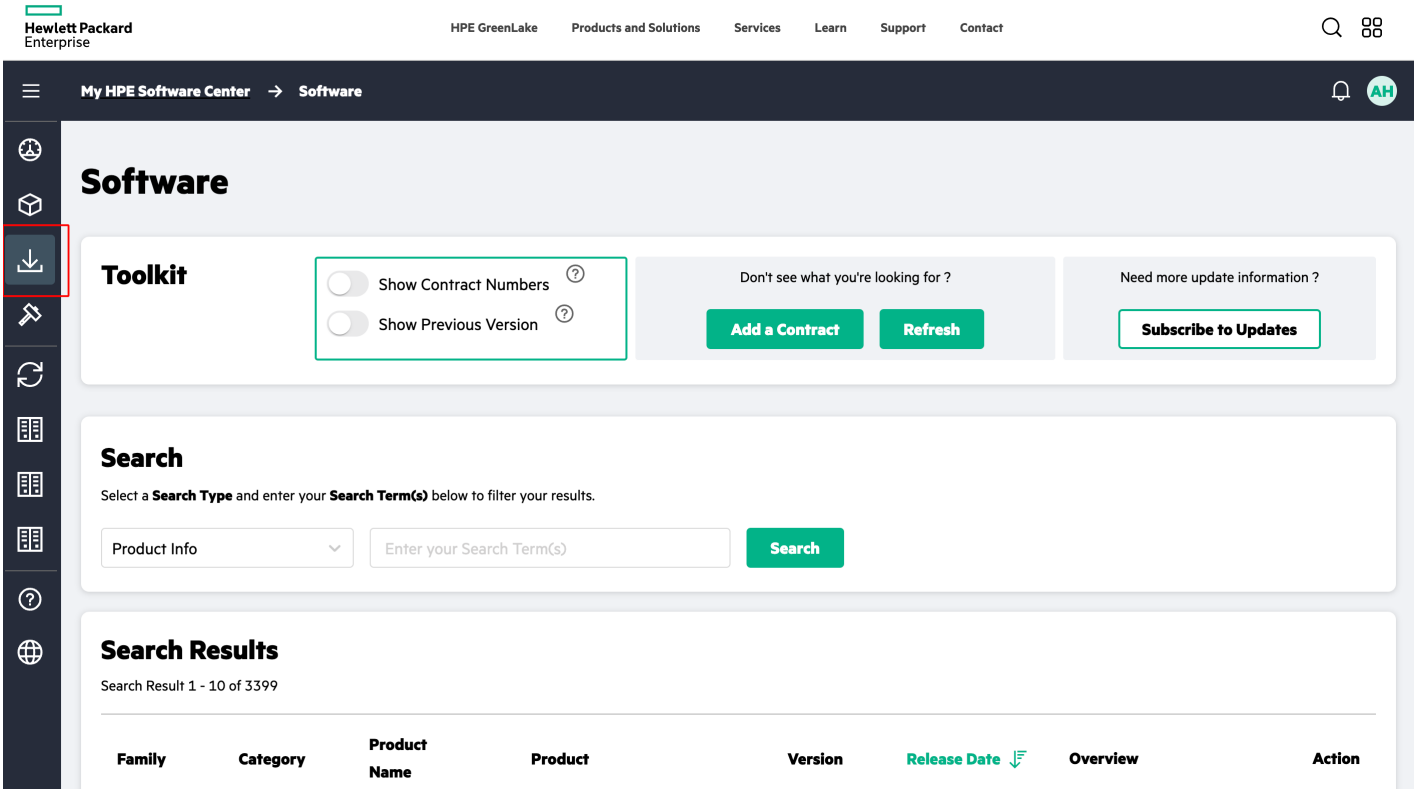


IMPORTANT

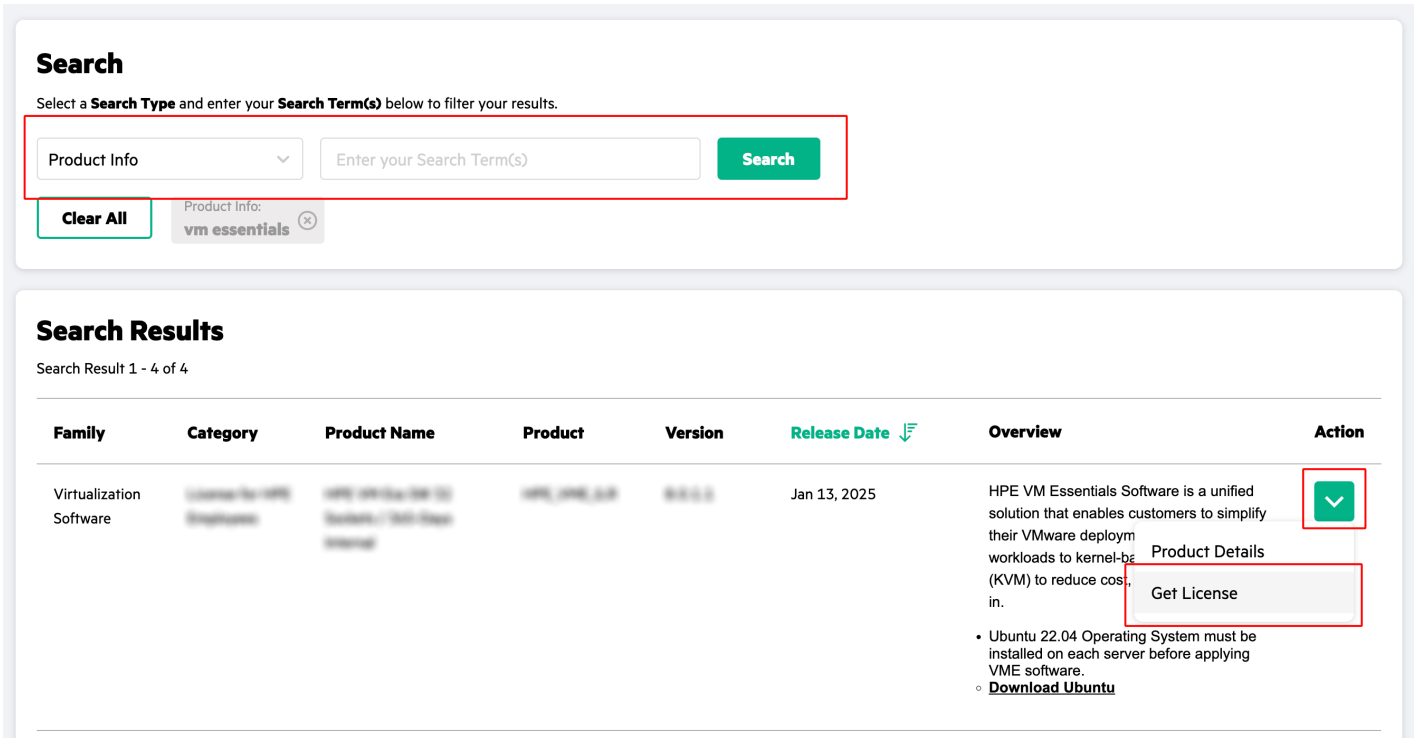
For those establishing clusters running Ubuntu 22.04, compatibility with GFS2 datastores requires hardware enablement (HWE) packages to be installed. This is a set of software components that enables users to run a longterm support version of Ubuntu yet still use newer hardware that might not be supported by the default kernel. Run `sudo apt install linux-generic-hwe-22.04` to install HWE packages. Some HVM Cluster layouts are compatible with Ubuntu 22.04 and these layouts are still supported but the latest ones are not.

Begin the installation process in My HPE Software Center. You'll eventually need to either get a license for HPE Morpheus VM Essentials Software or you'll need to access software entitlements in My HPE Software Center for a pre-existing license. If you don't have a permanent license available immediately on installation, a short-term evaluation license will be applied for testing purposes. A permanent license may be applied at any time after installation. The screenshots below describe the process for requesting a license but this may not be necessary if you already have one. Consult with your account manager if you have any questions.

Once logged into My HPE Software Center, click on the “Software” section from the side navigation.



Within the “Software” section, search for HPE Morpheus VM Essentials Software amongst your other software entitlements. A “Product Info” type search for the term “HPE Morpheus VM Essentials Software” may work but depending on the entitlements present in the account and future changes to search functionality, a slightly different search might be required. Once VM Essentials is successfully returned, click on the dropdown menu under “Action” and click on “Get License.”



From the download page, you'll see software packages, open source packages, and license files. For a fresh installation, you'll need both the HVM OS Install ISO and the HPE VM Essentials SW Image ISO. The HPE VM Essentials SW Image ISO contains a QCOW2 image containing the VM Essentials Manager. This ISO also contains a small Debian package which is required only if installing from vanilla Ubuntu rather than from the provided HVM OS. Mark the box next to any files you wish to download and then click “Download.” You do not need the separate debian packages offered outside of the `.iso` image as those are only for upgrading a pre-installed VM Essentials manager.

HPE_VM_Essentials_8.0.8_HVM_Installer_2404_S5Q83-11030.iso (4.29 GB)
SHA256 Checksum: d4299a5dd1fb60c708f83fc8febf17a5041e85417f04b7b12a... (Copy)
Signature File: S5Q83-11030.iso.sig

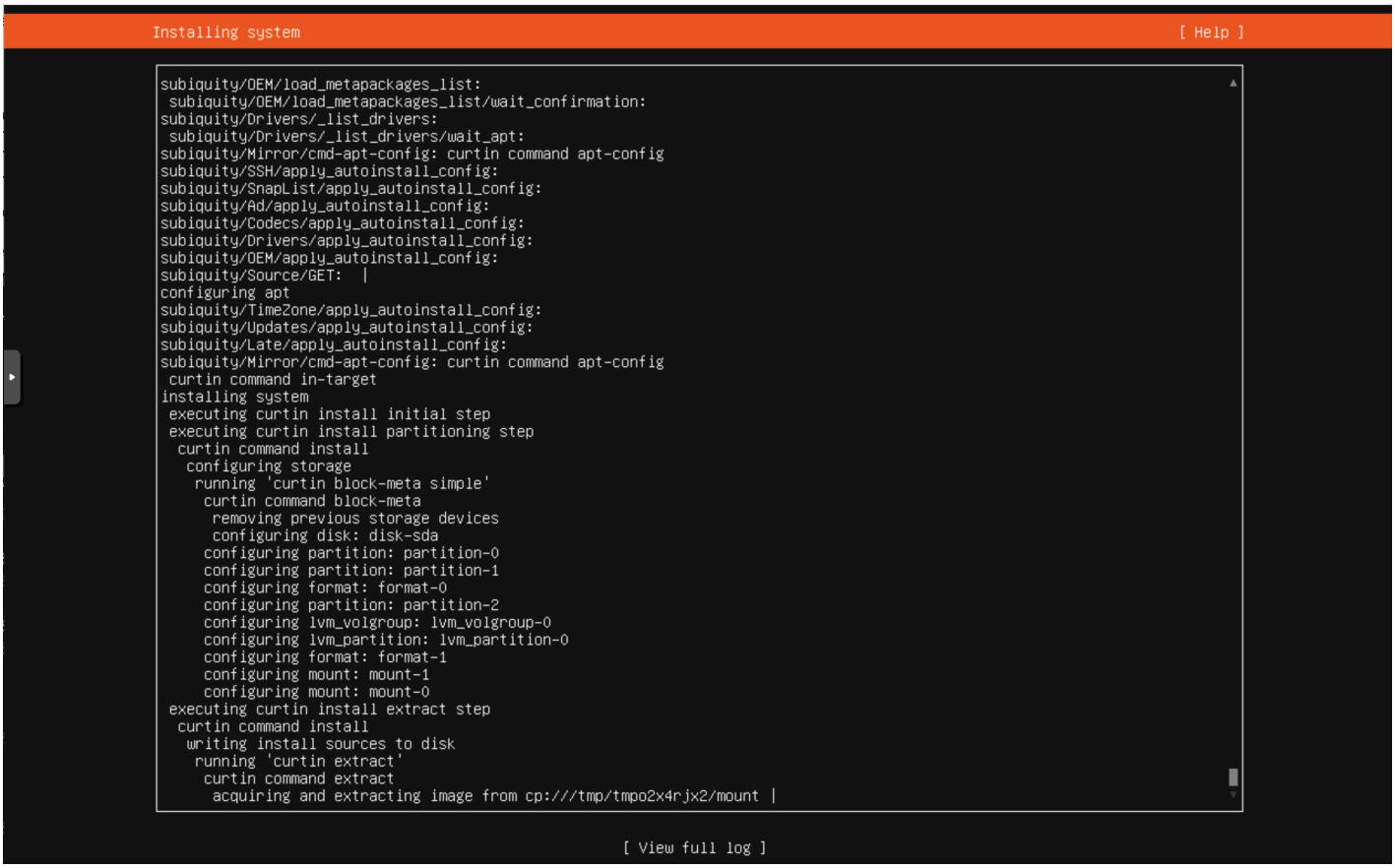
Your download speed may be affected by your internet service provider (ISP). Download curl Copy

NOTE
Some commands listed in this installation guide will require superuser privileges.

We'll install HVM on all host nodes first. Mount the HVM OS Install ISO to a DVD Drive device on the host machine and boot from it. Once successfully booted, select the option to install HVM OS.

GNU GRUB version 2.12
*HVM Install 24.04
Ubuntu Server with the HWE kernel
Test memory
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.
The highlighted entry will be executed automatically in 5s.

Proceed through the installer keeping in mind the Ubuntu network settings, Ubuntu storage settings, and external storage recommendations given in earlier sections of this install guide. Once details are entered for the initial account creation, proceed through the installation and reboot each host.



> **IMPORTANT**
>
> Tight time sync is vital for successful operation of an HVM Cluster. Take a moment to configure NTP server settings on each host. See **this knowledge article** for specific steps on configuring NTP for HVM Hosts.

Now that the host system has been installed, ensure the image is up to date by running `apt update -y && apt upgrade -y` as a super user. Now you can mount the HPE VM Essentials SW Image ISO to your computer. The exact process will vary by software platform. On Linux, first select a temporary mount point (such as `/mnt/iso`) or create a temporary mount point if it doesn't exist (`sudo mkdir /mnt/iso`). Next, mount the ISO to your temporary mount point (`sudo mount -o loop /path/to/file.iso /mnt/iso`). Take stock of the files by changing into the proper directory (`cd /mnt/iso`) and listing them out (`ls`).

Now that the files contained in the ISO are accessible, copy the QCOW over to one of the hosts. This will be the host that runs the HVM Manager VM. If you've installed vanilla Ubuntu, you will also need to copy over the `hpe-vm` Debian package to all hosts (though this is not necessary if you've installed HVM OS). On Linux, this could be done with `scp` (`scp /path/to/file.qcow2 username@hpevmhost_hostname_or_ip:/path/to/desired/location/`) but the copy process will be slightly different for other operating system platforms.

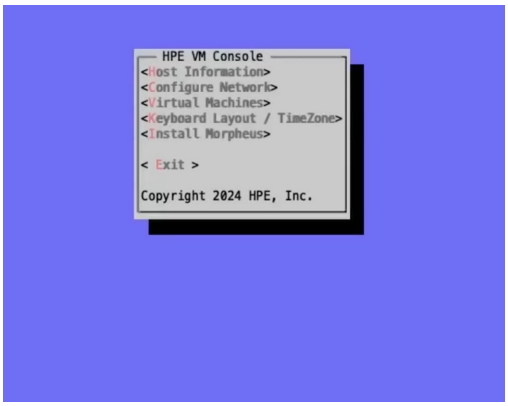
If necessary, go ahead and install the `hpe-vm` Debian package with `apt install -f hpe-vm.deb`. The "-f" option indicates that a file will be installed. Note that the Debian file name listed here is an example placeholder and the name of your downloaded file will likely be different. When asked if you wish to install all of the packages provided, confirm that you do and then wait for installation to complete. This process is installing on the host all of the packages needed to be part of a virtualization server, including KVM, Libvirt, and more. HVM OS includes these packages preinstalled so this installation step is unnecessary if you installed HVM OS rather than vanilla Ubuntu.

> **IMPORTANT**
>
> The rest of this section describes the configuration process within the console for a specific network configuration. Your network configuration may be different and certainly interfaces and VLANs will be differently named. This is meant to illustrate the tools that are available within the console for performing various networking configurations. You may or may not need all of these steps and the specific configurations within these steps may be different in your environment.

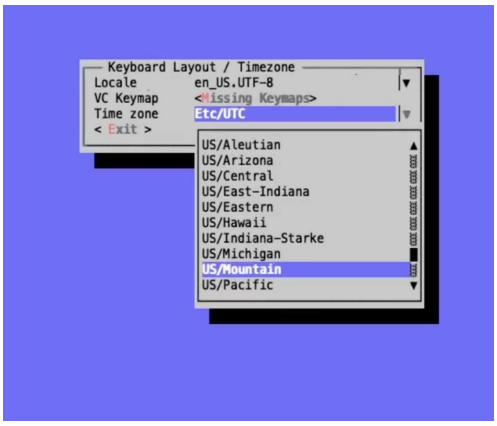
With that, HVM OS and the VM Essentials console installation is complete. Enter the console with the following command: `hpe-vm`.

NOTE

Some versions of the installer also include an option to install the VME worker. The VME worker is meant for sites where direct SSH communication between the HVM hosts and the VM Essentials manager is not possible. It is a feature of HPE Morpheus Enterprise Software and SimpliVity, it is not compatible with HPE Morpheus VM Essentials Software. More information on distributed workers is available in **HPE Morpheus Enterprise documentation**.



First, enter the section for keyboard layouts and timezones. Set the time and make any changes to the keyboard layout, if needed.

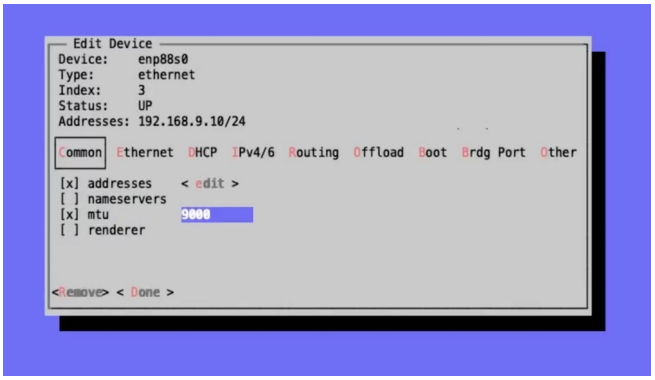


Next, enter the section for network configuration. The first thing that I'm going to do is set the MTU for relevant interfaces to 9000 (jumbo frames). This has a number of benefits including improved efficiency, reduced latency, and optimization for storage networks. Open the "Device Type" dropdown and choose "vlan". In my example case, there's one VLAN which is the "bond0.2" VLAN shown in a prior section. Once selected, mark the box next to "mtu" and enter "9000" in the resulting box. Then, save changes.

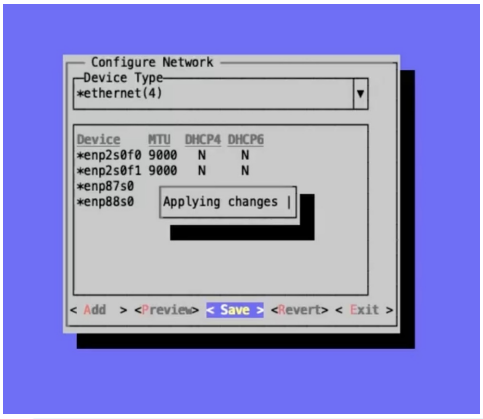
Next, use the "Device Type" dropdown to once again select "ethernet" which you saw earlier before switching into the "vlan" section. Using the same process, I will also set the MTU to 9000 on both ethernet devices that make up my bond as well as on the bond itself. To get to the bond, you'd access the bond section from the "Device Type" dropdown in the same way that VLANs and ethernets were accessed. Now that I've set MTU of 9000 across the board, I'll go back to the ethernets section to work with my other two devices (the storage interfaces).

I'll continue this example by opening each of the two storage interfaces in turn. Three configurations I'll point out here are "addresses", "nameservers", and "mtu". In this case, I'll mark the box for "addresses" and provide an address in the pop-up modal that appears. I don't need to make any other configurations within that modal (lifetime, etc). A nameserver is not needed because the storage network are isolated and don't need to route out anywhere. Finally, I'm marking the box for "mtu" and setting the value at 9000 as I have with other interfaces. Next, tab over the DHCP section and disable DHCP for this interface. Save the changes and repeat the process for the other

storage interface.



Once all of the necessary networking configurations are made, you'll want to save all changes. This will cause the changes to be applied and take us back to the main screen where we first accessed the timezone section and the networking configuration section. The console will show you that changes are being applied and will respond with a confirmation if they are successful.



IMPORTANT

In an earlier section, we discussed network bond types, one of which was active/backup. If using active/backup bonds, it's important to note that a default MII polling setting is not applied out of the box. This means failover won't work correctly without configuring it yourself. Take a look at **this knowledge article** for specific steps to configure this in `netplan` and the `hpe-vm` console.

At this point, I am done configuring my example interfaces through the VM Essentials console. It does have some additional functionality not shown here which may be needed depending on your specific network configuration. Make sure to complete this process on all hosts before moving on to the next section which covers the installation of VM Essentials manager onto one of the prepared HVM hosts.

Manager Installation

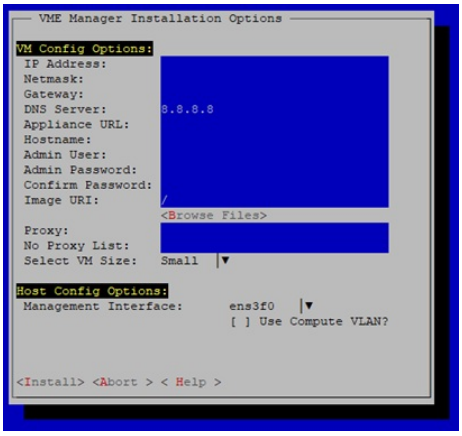
Having configured the HVM hosts through the VM Essentials Console in the prior step, we'll now install VM Essentials manager. Unlike the console, the manager is only installed on one of the hosts and serves as the control plane for the server in addition to providing a provisioning engine, automation functionality, monitoring, secrets management, and a lot more. Before starting, make sure you've already downloaded the QCOW image for the manager and are aware of its full path on the host you've chosen to work from. In fact, it may be beneficial in the next step to go ahead and copy the full path into your paste buffer. The image is available in the HPE software center. Contact your account representative if you are unable to download it using the steps in the previous section.

Before you begin, the following information should be readily at hand:

- IP address to give to the VM Essentials manager
- URL for the web server
- DNS resolution for the URL (points the URL to the manager IP address)
- VLAN the manager should be deployed on
- Management interface name
- Compute interface name

To install the manager, select "Exit" if in a configuration modal or use the `hpe-vm` command as superuser and select "Install VME

Manager". Here we are given a modal containing some configuration options required for the VM Essentials manager.



Let's first configure the following fields using the information mentioned previously. You should have available for this step:

- IP Address
- Netmask
- Gateway
- DNS Server
- Appliance URL
- Hostname (same as the appliance URL without the FQDN)

In the "Image URI" field, enter the "Browse Files" option to traverse your filesystem and locate the QCOW2 image. Once found, select the file and then select "Open". The image path will then appear in the "Image URI" field. Alternatively, paste in the path to the manager image.

NOTE

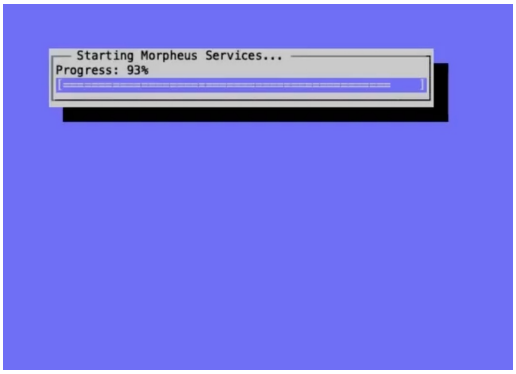
Once a host is initially set up over SSH, communication to the VM Essentials manager is mostly handled through an outbound connection from an agent running on the host to the Manager VM. This makes the Appliance URL configuration very important. This is the HTTPS URL the agent will connect to from within each hypervisor host. The one exception are hypervisor console sessions which still go through SSH.

After filling in those fields, enter a username and password for an SSH user that can be used to get into the manager machine. Following that, if necessary, configure any proxy details.

The final configuration to make here involves specifying the size of the manager machine, either small, medium, or large. Each of the respective sizes consumes the following amount of resources:

- **Small:** 2 vCPUs and 12 GB RAM
- **Medium:** 4 vCPUs and 16 GB RAM
- **Large:** 4 vCPUs and 32 GB RAM

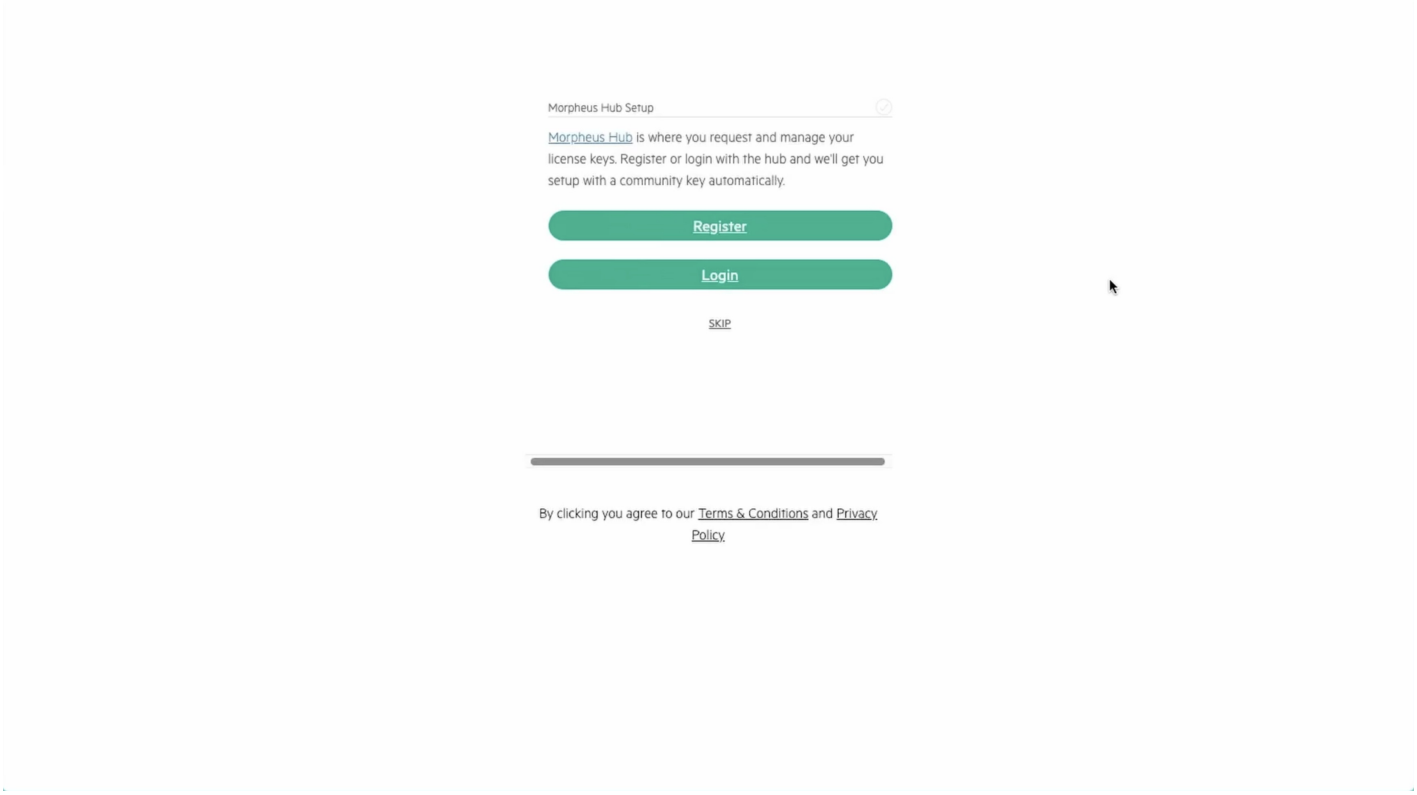
The greater the capacity, the greater amount of resources and cluster sizes the VM Essentials manager can manage. For large production environments, it's recommended you select a large manager. After selecting the size, you'll need to identify the management interface and (if using) the compute interface and compute VLAN tag. Following all of these configurations, select "Install".



At a certain phase in the install process, you'll see a message in the progress bar modal stating "Starting Morpheus Services...". At this point, you can direct a web browser to the appliance URL and see if you can access the appliance. If you get a response returned, even if it's just telling you the appliance is still loading, that's a good sign the web server is installed and things are working. Once all is well, you will arrive at a setup page which leads us into the next section on setting up VM Essentials manager.

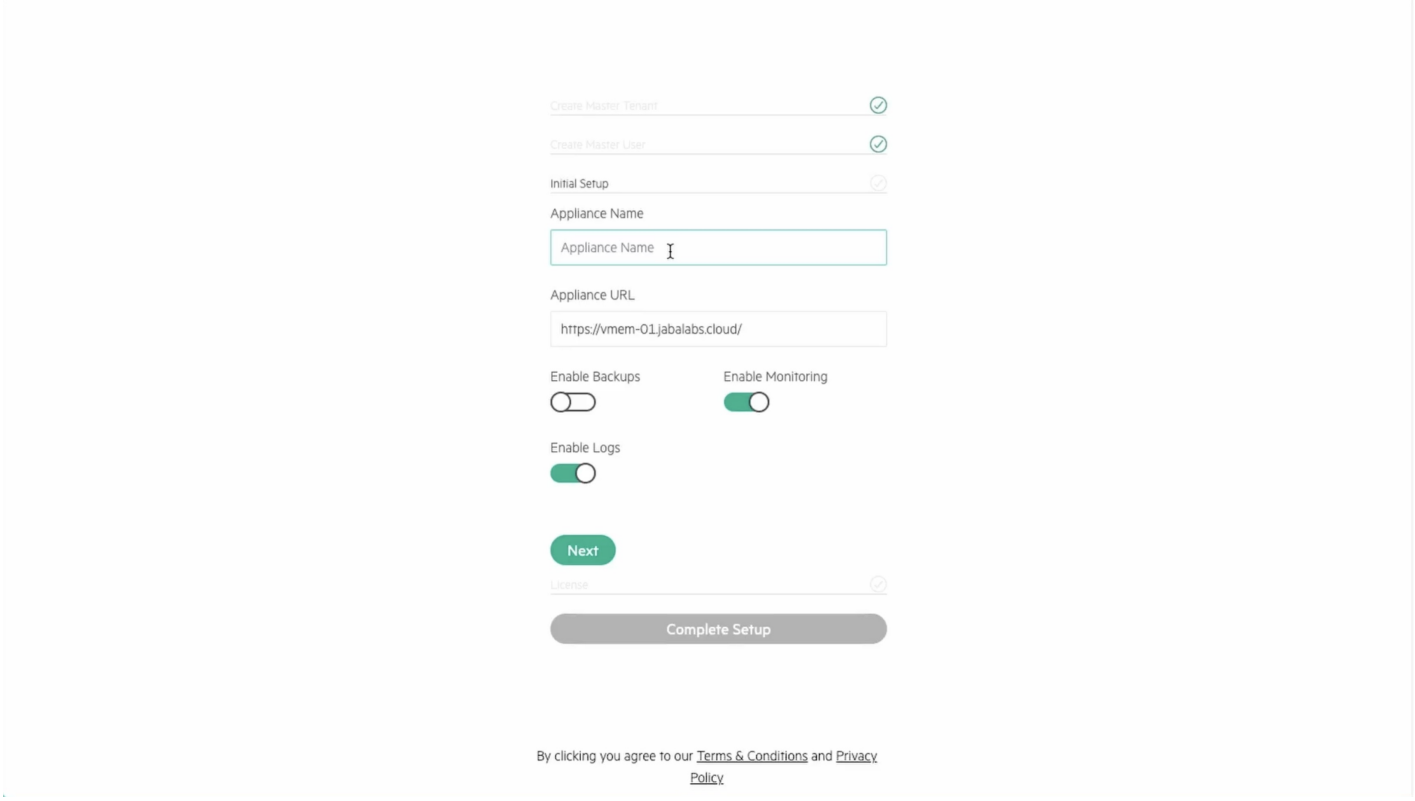
Manager Initialization

With VM Essentials manager up and running, you can now access the UI frontend by pointing your web browser to the appliance URL that you set in a previous step. You should see a registration screen like the one below.


Morpheus Hub Setup
Morpheus Hub is where you request and manage your license keys. Register or login with the hub and we'll get you setup with a community key automatically.
Register
Login
SKIP
By clicking you agree to our Terms & Conditions and Privacy Policy

You'll need a license to go much further with the product. If you've followed this guide up to this point, you should already have your license key downloaded from My HPE Software Center. If not, you can log back in any time an re-download the file containing the license key. If you choose to skip entering a license key at this time, a short-term evaluation license will be applied. This can be upgraded to a full license at any time from the global settings section of the application.

The rest of the process involves naming the account on the manager and entering the details for your initial administrator user. Next, provide a name for the appliance, confirm the appliance URL is correct as entered, and choose from a few global enablements (for backups, monitoring, and logs).



After clicking through to the next section, you will paste in your license key. Click “Complete Setup” and you will be dropped into the UI for the first time. Installation is now complete!

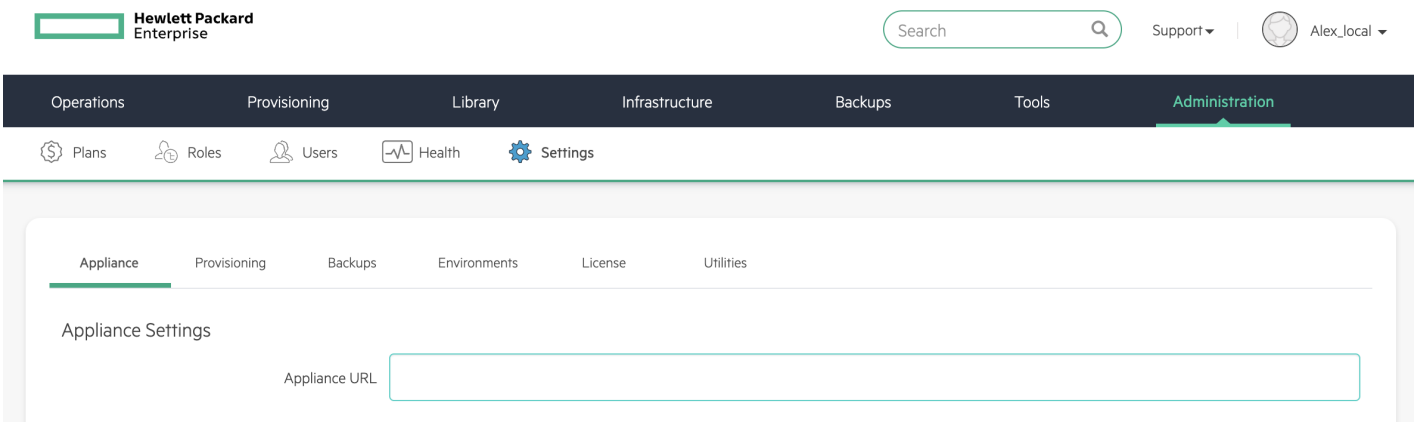
At this point, you are ready to move on to the next section which goes over the initial environmental setup steps that must be undertaken to add the first HVM cluster to the VM Essentials manager.

Initial VM Essentials manager Setup

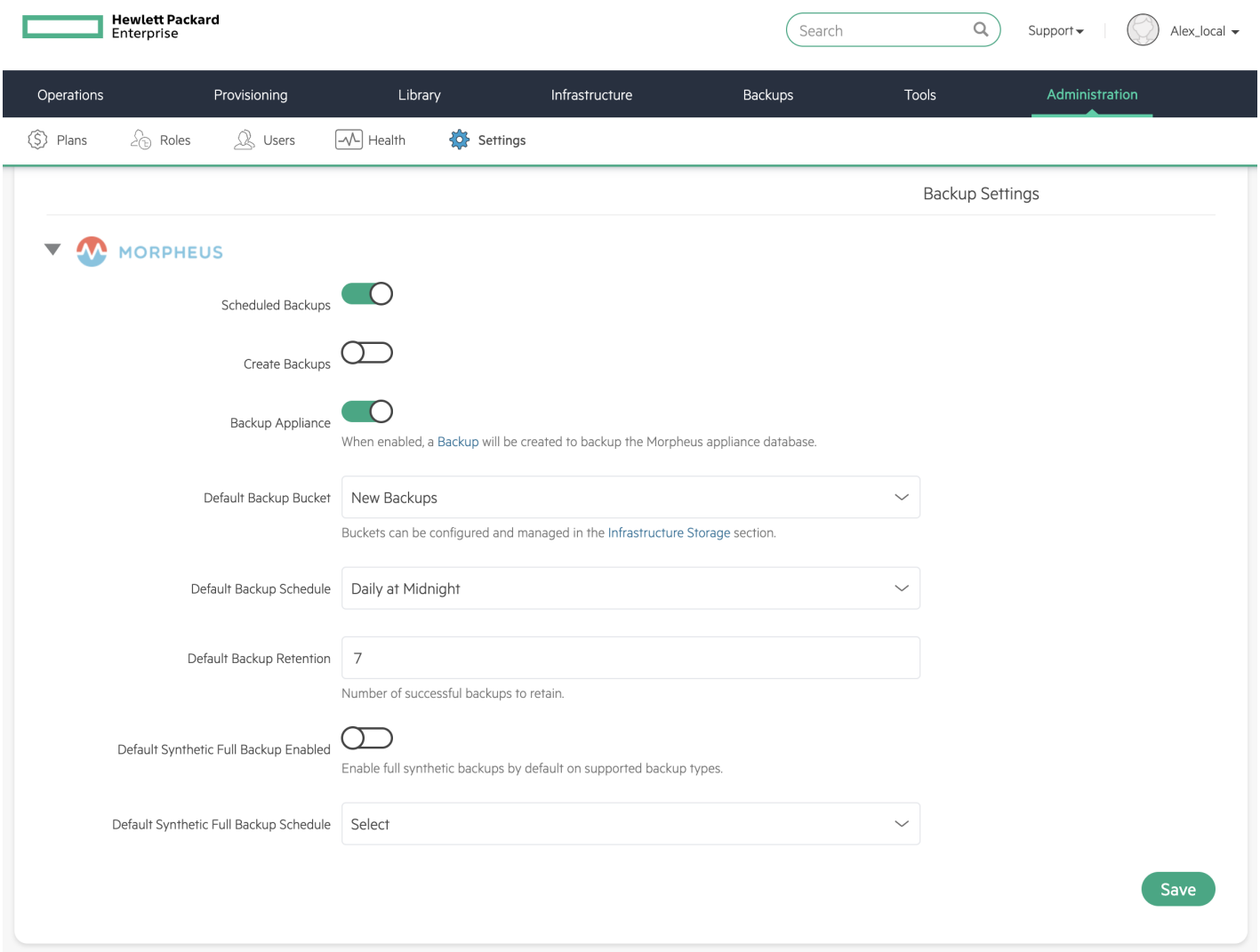
With VM Essentials manager now installed, you’re dropped into the UI and want to get up and running as quickly as possible. This section goes over some useful first steps for configuring the environment, locating useful features, and adding the first HVM cluster.

Global Settings

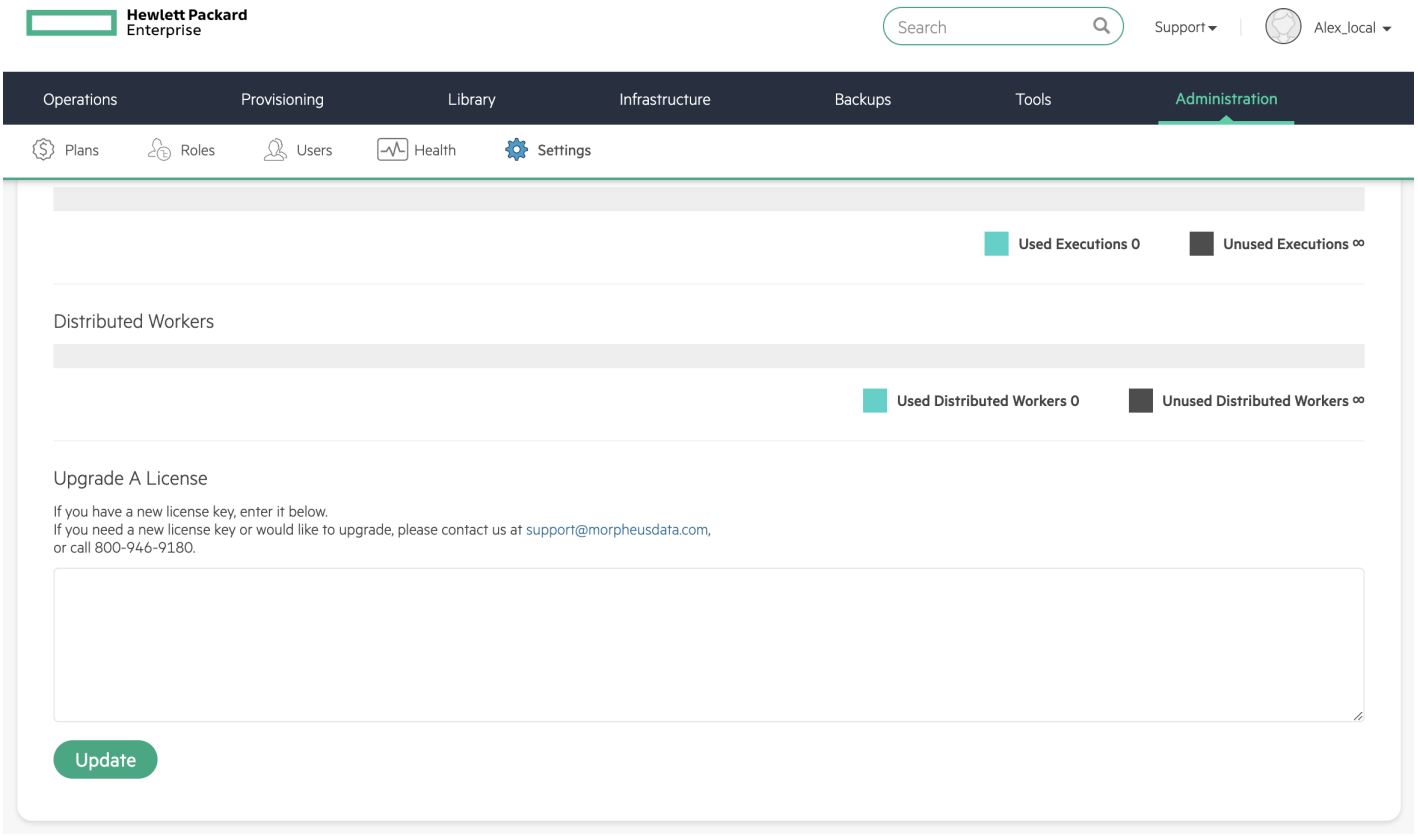
A useful first stop is in global settings (Administration > Settings). Within the Appliance category, check and fill an “Appliance URL” value. This is the default value for VM Essentials Agent installation and functionality. All Instances and hosts must be able to resolve and reach this URL over port 443 for the Agent to install and function properly. Individual Clouds can also have an individual Appliance URL which supersedes the global one set here. While here in the Appliance category, consider checking the “Skip Agent Install” toggle. If on, this toggle will be set by default in the Instance provisioning wizard. If off, this toggle will not be set by default in the Instance provisioning wizard. If your default stance is to install the Agent and maximize the value provided for workloads running on HVM clusters, this toggle should be off.



Next, check the Backups section which houses global settings related to backups. If “Scheduled Backups” is toggled, default automatic backup settings will be pre-set each time you begin to configure a new Instance through the Instance provisioning wizard. These default backups will target the default bucket, schedule, and retention settings you see here. This is a good time to double check your default backup bucket and retention settings as it is possible to backup Instances directly to the VM Essentials manager VM. If you fill the Manager’s disk with backups you could bring the Manager down.



One last area to check is the License section. Here you can check your usage against licensed maximums as well as apply new licenses. If you started the Manager using the built-in trial license you will have to return here at some point to apply a full license.

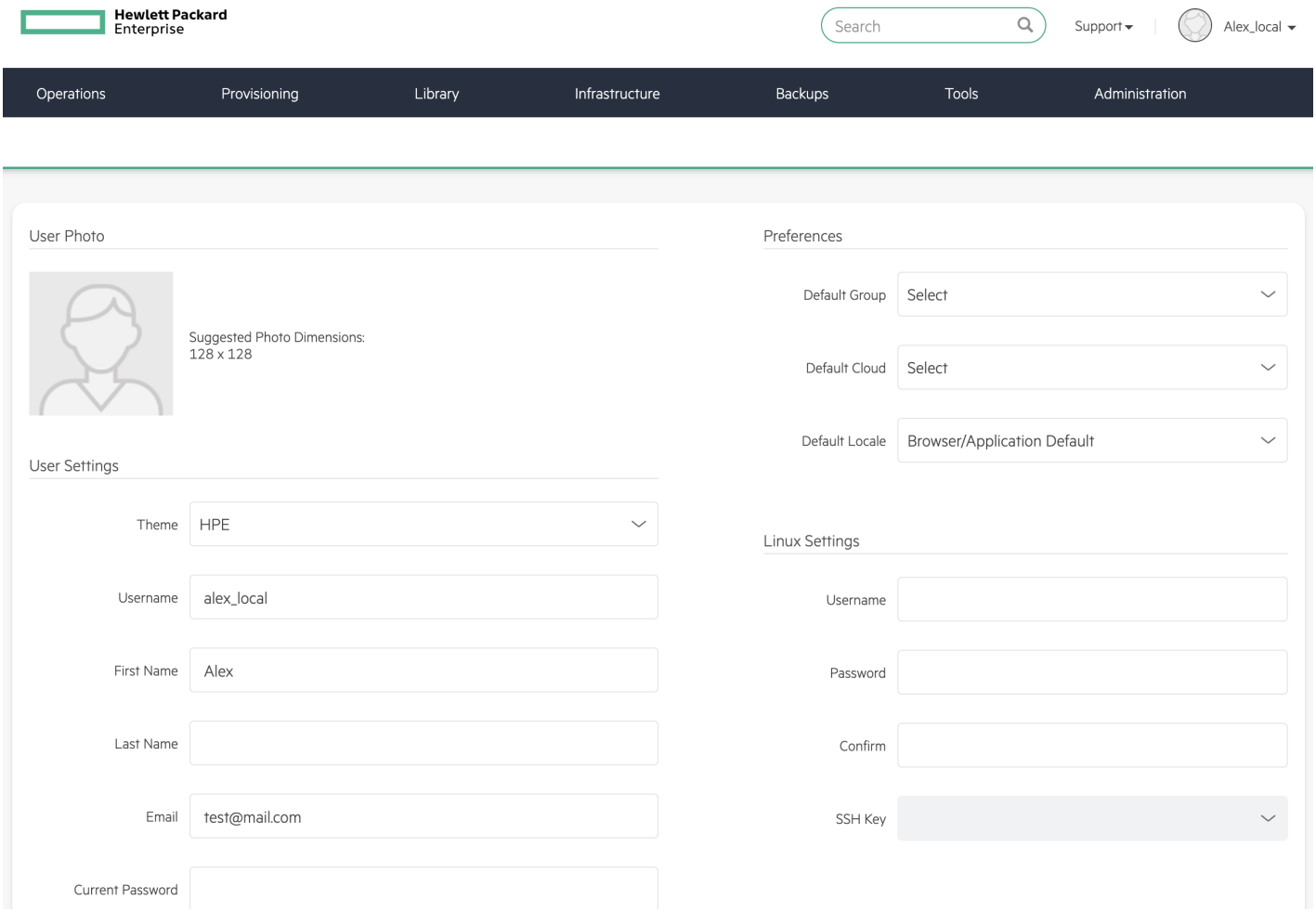


See the **global settings section** of VM Essentials documentation for complete details on settings.

User Settings

Next, check User Settings. User Settings is accessed by clicking the user's name in the upper-right corner of the application window and then clicking "USER SETTINGS".

Some settings you may want here include "Email" which will ensure any automatic email generated by the Manager (such as Instance provisioning success messages) arrives at a place it can be seen. Setting a default Group and Cloud is also useful as new workloads will begin with your most-used Group and Cloud set by default, which will save a lot of clicks over time. If you haven't yet created your first Group and Cloud (covered in a later section), come back later to set that default. Finally, it's useful to configure a Linux and Windows user here. At provision time if you opt for your user to be added to provisioned Instances, a user will be added with your indicated username, password, and public key (if specified, you must have an existing SSH keypair in the Manager) for easy access to any running workload. API access settings and 2FA settings are also here.



Creating Groups and Clouds

You won't be able to add your first HVM cluster without a pre-existing Group and Cloud. Groups define logical groupings of resources and users access those resources based on the Groups associated with their Roles. A Cloud can represent a grouping of HVM clusters or a connection into a VMware vCenter environment. You can read more on Groups and Clouds **here** and **here**, respectively. This guide will go through the process of adding Private Cloud-type Clouds which house HVM clusters. For VMware-type Clouds, see the associated **integration guide**.

Start by making your first Group. Click + CREATE at Infrastructure > Groups. A Group needs only a name, at minimum. If this Group is going to hold some or all of your HVM clusters, you may want to name it accordingly. Once done, save the new Group. We'll next create a Cloud. Navigate to Infrastructure > Clouds and click + ADD. In addition to being a logical grouping for HVM clusters, Clouds can also be a connection into a specific VMware vCenter environment (as narrow as a specific Resource Pool or folder, or more broadly scoped). See the link in the previous paragraph for more details on VMware Clouds. In this case, create a "Private Cloud." Once again, a name is the minimal amount of information required and you may want to name this Cloud in a way that indicates which HVM clusters it will encompass. When done, save the new Cloud.

Creating the first HVM cluster

In preparing the environment, we've already prepped the physical cluster servers but now it's time to provision the actual cluster object within VM Essentials. Begin by navigating to Infrastructure > Clusters and click + ADD CLUSTER. Currently, the only available cluster type is "HVM," which is what we want. Select the correct cluster type and click NEXT. On the Group tab, select the Group we created in the previous section and click NEXT. On the Name tab, select the Cloud we created in the previous section and enter a name for the cluster. Click NEXT.

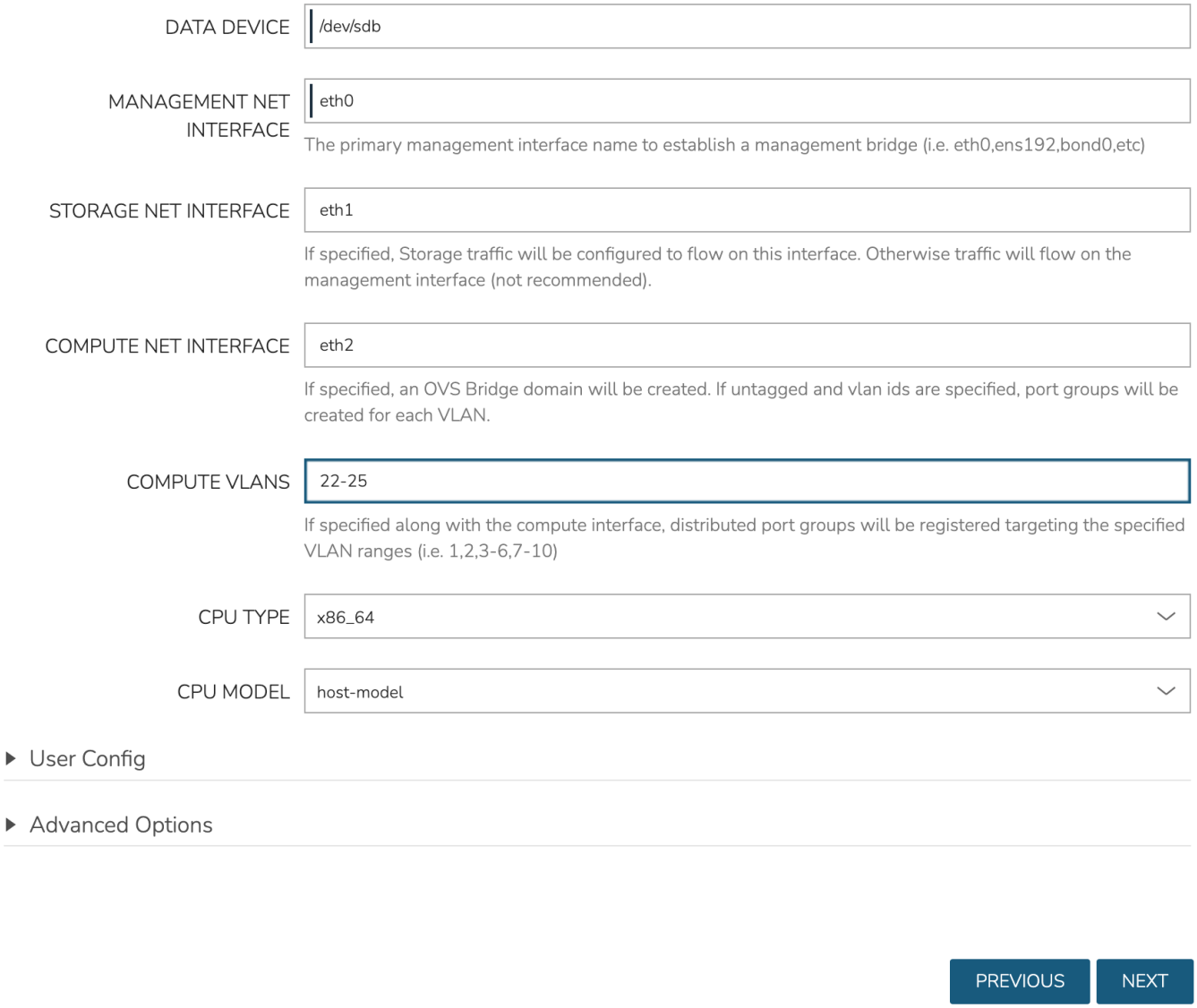
VM Essentials gives the option to select a hyperconverged infrastructure (HCI) **LAYOUT** or non-HCI. In this example, the HCI Layout is used (requires a three-node minimum). Next, configure the names and IP addresses for the host boxes (**SSH HOST**). The SSH HOST name configuration is simply a display name in VM Essentials, it does not need to be a hostname. By default, configuration space is given for three hosts which is what this example cluster will have. You must at least configure one and it's possible to add more by clicking the (+) button. The **SSH PORT** is pre-configured for port 22, change this value if applicable in your environment. Next, set a pre-existing user on the host boxes (**SSH USERNAME** and **SSH PASSWORD**) and **SSH KEY**. Use a regular user with sudo access.

In the next part of the modal, you'll configure the storage devices and network interfaces. When storage initializes, it needs to be pointed to

an initial data device. Configure this in the **DATA DEVICE** field. At this time, only one device may be given but in the near future, an update will allow for multiple devices to be configured which would be added to the total storage as one large volume. Find your disk name, if needed, with the `lsblk` command. In my case, the target device is located at `/dev/sdb`.

Though not strictly required, it's recommended to have separate network interfaces to handle cluster management, storage traffic, and compute. In this example case, `eth0` is configured as the **MANAGEMENT NET INTERFACE** which handles communication between the cluster hosts. `eth1` is configured as the **STORAGE NET INTERFACE** and `eth2` is configured as the **COMPUTE NET INTERFACE**. The **COMPUTE VLANS** field can take a single value (ex. 1) or a range of values (ex. 22-25). This will create OVS port group(s) selectable as networks when provisioning workloads to the cluster. If needed, you can find your network interface names with the `ip a` command.

Finally, only one **CPU TYPE** is currently supported (`x86_64`) though this may change in the future. For **CPU MODEL** configuration, we surface the entire database of model configurations from `libvirt`. If unsure or if you don't know of a specific reason to choose one or the other, select `host-passthrough` which is the default option.


DATA DEVICE
/dev/sdb
MANAGEMENT NET INTERFACE
eth0
The primary management interface name to establish a management bridge (i.e. eth0,ens192,bond0,etc)
STORAGE NET INTERFACE
eth1
If specified, Storage traffic will be configured to flow on this interface. Otherwise traffic will flow on the management interface (not recommended).
COMPUTE NET INTERFACE
eth2
If specified, an OVS Bridge domain will be created. If untagged and vlan ids are specified, port groups will be created for each VLAN.
COMPUTE VLANS
22-25
If specified along with the compute interface, distributed port groups will be registered targeting the specified VLAN ranges (i.e. 1,2,3-6,7-10)
CPU TYPE
x86_64
CPU MODEL
host-model
User Config
Advanced Options
PREVIOUS
NEXT

At this point we've kicked off the process for configuring the cluster nodes. Drill into the Cluster detail page and click on the History tab. Here we can monitor the progress of configuring the cluster. VM Essentials will run scripts to install KVM, install OVS, and to prepare the cluster. In just a short time, the cluster provisioning should complete and the cluster will be ready to deploy workloads.

For more on cluster provisioning, monitoring clusters, and provisioning workloads to existing clusters, see the full section on HVM Clusters.

Take Note of Virtual Images and Automation

Now that we have a cluster, let's take a quick look at where Virtual Images live and where Automation scripts can be created and stored. Both are under the Library menu. In the Virtual Images section is a list of all Virtual Images that have been synced from integrated Clouds (such as a VMware vCenter Cloud) or manually uploaded. Additionally, running workloads (such as VMs running on HVM clusters) can be saved as images with one click. Once the image has been taken, it will appear in the list of Virtual Images here. When provisioning, a list of all compatible images for the target Cloud type is shown. You will need to have at least one HVM-compatible image here in order to provision new Instances to the cluster. When uploading images manually, there's often some additional configuration that must be done to make the

image compatible with the intended target Cloud type. Take a look at **Virtual Images** documentation for more detail.

Next in the Library section is Automation. This page contains a list of automation scripts that are stored in VM Essentials. These scripts can be shell scripts, Powershell scripts, or a restart Task that restarts workloads it's run against. I won't go into full detail on writing scripts and the nuances of how they can be used in this section but there's more in the full **Tasks section** of VM Essentials documentation. Tasks can be used on the Automation tab of the Instance provisioning wizard. Stack Tasks and chain the results for fully automated Instance deployment.

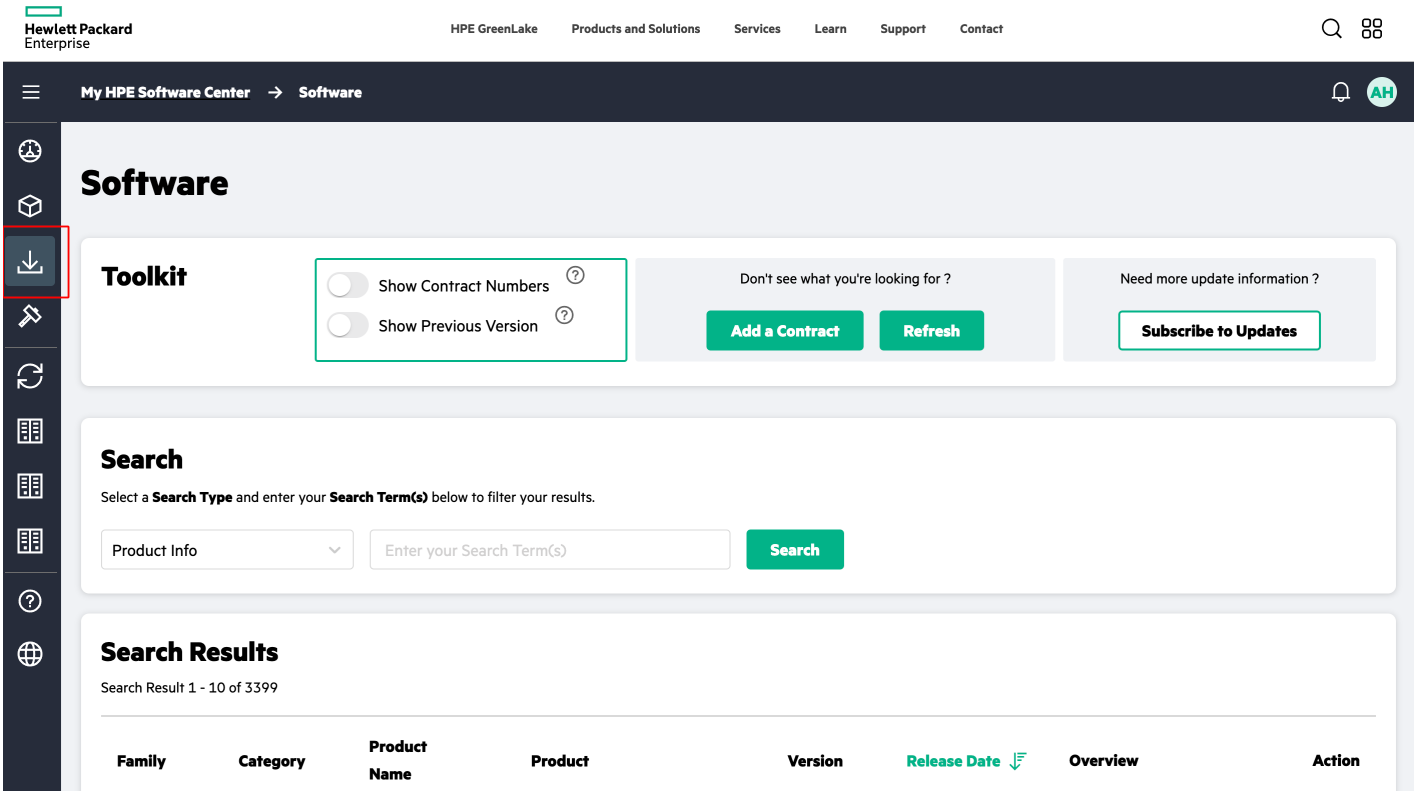
Provsioning the First Workload

All groundwork is now laid to begin provisioning workloads to the HVM cluster. Launch the wizard by going to Provisioning > Instances and clicking + ADD. Select an HVM-type Instance and click NEXT. You'll once again notice the Group and Cloud we created in this guide can be selected. You'll also specify a plan (VM size), resource pool (cluster), image, and cluster host, among a few other selections. After clicking NEXT, you'll land on the Automation tab where a set of Tasks can be selected to automate the deployment and configuration of the new Instance. Once the wizard is fully completed, a new Instance will be provisioned to the HVM cluster. You are now ready to add more of your images, add more automation tasks, and monitor workloads that are running on your clusters.

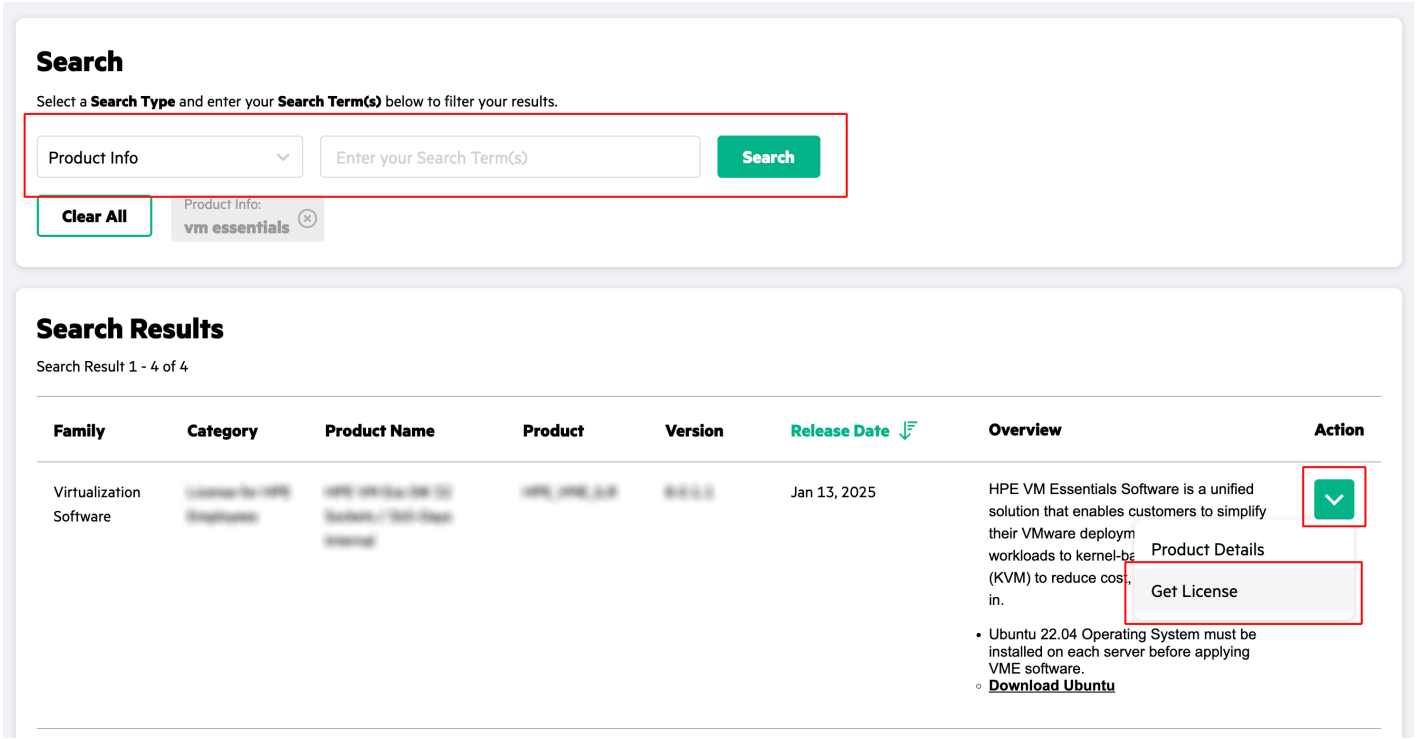
Upgrading the Manager

To upgrade the VM Essentials manager, you'll need to obtain the `.deb` upgrade package(s) from the HPE Software Center. Reach out to your account manager if you're unable to access the downloads as described in the next paragraphs. For an upgrade, you'll need the debian package (not the ISO, which is for first-time installation). If you are performing an offline upgrade, you will also need the "supplemental" debian package.

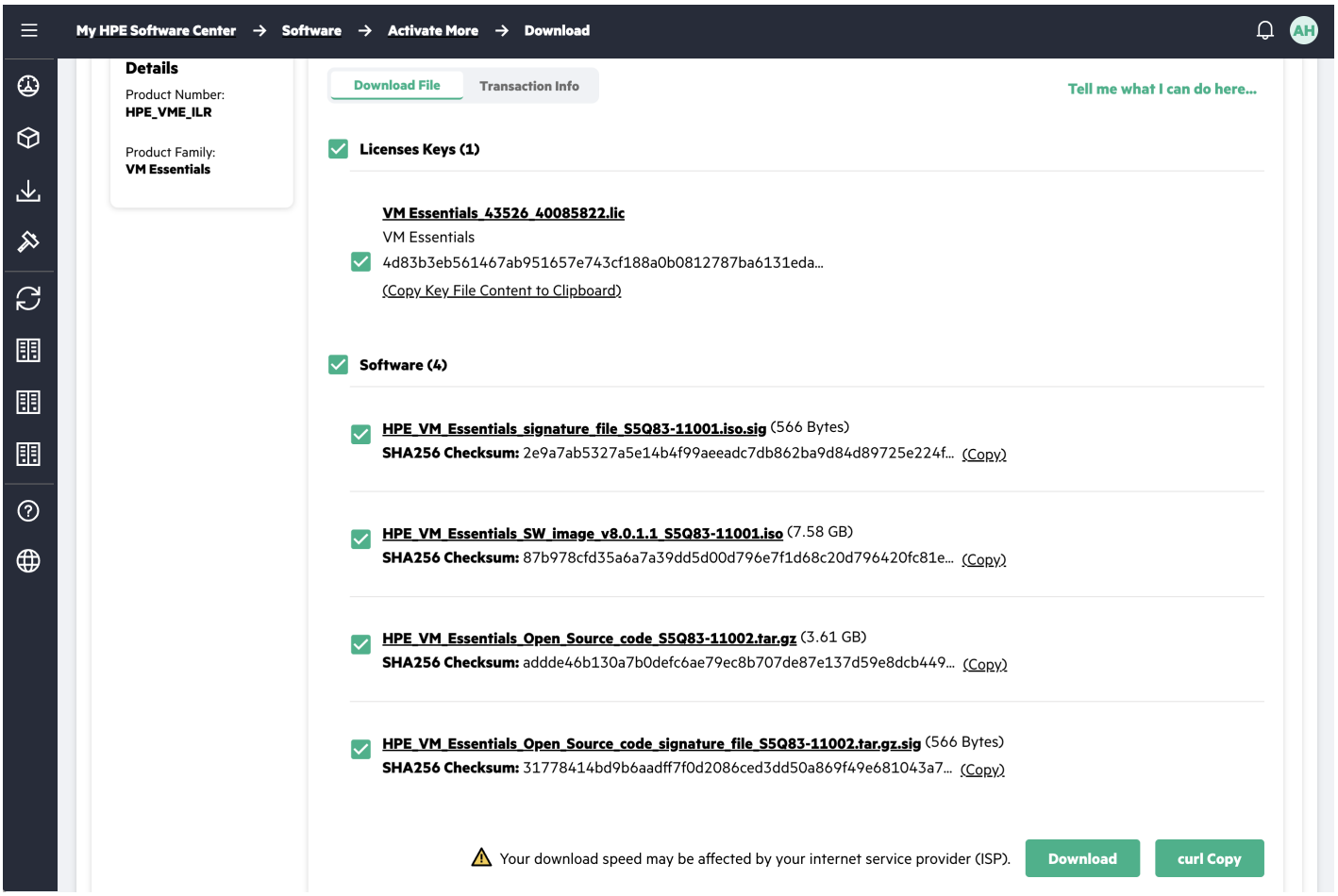
Once logged into My HPE Software Center, click on the "Software" section from the side navigation.



Within the "Software" section, search for HPE Morpheus VM Essentials Software amongst your other software entitlements. A "Product Info" type search for the term "HPE Morpheus VM Essentials Software" may work but depending on the entitlements present in the account and future changes to search functionality, a slightly different search might be required. Once VM Essentials is successfully returned, click on the dropdown menu under "Action" and click on "Get License."



From the download page, you'll see software packages, signature files and license files. Mark the checkbox next to any that you need and download them to your computer.



For an upgrade, we only need the `.deb` file available in the software center (and potentially the "supplemental" debian package as well if this will be an offline upgrade). To continue, copy the `.deb` file(s) over to the VM Essentials manager VM. On Linux, this could be done with `scp` (`scp /path/to/file.deb username@<VM IP address>:/path/to/destination`). You'll need the VM user's password unless you're using SSH keys. Alternatively, you may also click the "curl Copy" button to download a .txt file containing a curl command which you can paste into a terminal session connected to the HPE Morpheus VM Essentials Manager VM.

With the `.deb` file in place, we need to open a console connection to the VM Essentials manager VM to perform the actual upgrade. There

are a number of methods to accomplish this but below are two examples from either an HVM host or from your own computer.

Subtopics

- Setup from the HVM host
- Setup from another computer
- Upgrading

Setup from the HVM host

Confirm the manager VM name (`virsh list`) and connect with `virsh console <vm name>` . This starts a local VNC serial connection. This method only works if the host has GUI capabilities installed, which means the host must be running Ubuntu Desktop or Ubuntu Server with GUI services installed.

Setup from another computer

Confirm the manager VM name (run `virsh list` on the HVM host). Next, make note of the VNC port and password for the VM Essentials manager VM. This is done by running `virsh edit <vm name>` on the HVM host and finding it within the block beginning `<graphics` . This block is typically near the bottom of the XML. Having obtained this information, move back over to your own computer (must be a computer with a desktop terminal, access to the VME host, and GUI capabilities). Connect to the SSH tunnel: `ssh -L <VNC PORT>:127.0.0.1:<VNC PORT> <VME Host User>@<Host IP/hostname>` . Then, using a VNC viewer (for example, VNCViewer64), connect to `localhost:<VNCPort>` . Use the password obtained from the VM XML viewed earlier.

Upgrading

Having copied over the needed files and connected to the VM Essentials manager VM, the upgrade is completed in just a few commands. These commands will stop the current services, install the package, and then reconfigure the Manager. Replace the placeholder `.deb` file in the commands below with the correct path and file name of the package you've copied over.

> **IMPORTANT**
>
> Upgrading VM Essentials manager will result in downtime of at least a few minutes. Ensure users are not doing critical work during the upgrade window. This downtime applies only to the Manager itself and has no effect on the hypervisor host(s) or any provisioned VMs currently running.

```
sudo morpheus-ctl stop morpheus-ui
sudo dpkg -i xxxx.deb
sudo dpkg -i xxxx.supplemental.deb  # Optional -- Only for offline upgrades
sudo morpheus-ctl reconfigure
```

All services will automatically start during the reconfigure process. After the reconfigure has succeeded, tail the UI service to watch UI startup logs with `morpheus-ctl tail morpheus-ui` . Once the UI service is up and running, the upgrade process is complete. Attempt to reach your appliance normally through a web browser to confirm success.

> **NOTE**
>
> Services will be stopped during package installation and started during the reconfigure process, including the `morpheus-ui` service. If the reconfigure process is interrupted or fails, the `morpheus-ui` service may need to be manually started or restarted. In certain situations if another service hangs on starting during reconfigure, run `systemctl restart morpheus-runsvdir` then reconfigure and restart `morpheus-ui` if successful.

Following upgrade, it's advisable to check for any available HVM Host Agent upgrades. To upgrade the HVM Host Agent, navigate to an HVM Host detail page, expand the ACTIONS menu, and click "Upgrade Agent." This process must be repeated for each HVM Host that

makes up the HVM Cluster. Alternatively, you could also select "Download Agent Script" to download an Agent upgrade script which can be run when connected to the host through a terminal session. The Agent upgrade scripts are Host-specific so an individual script would need to be downloaded for each HVM Host.

Upgrade Compatibility Table

This section contains a table of compatible upgrade paths. The far left column contains the HPE Morpheus VM Essentials Manager version you're starting from. The columns to the right indicate versions compatible for upgrade from your starting version. If the version number is listed, it is a compatible upgrade path. If an "**X**" is listed instead, the upgrade path is unsupported.

From Version	To Version								
8.0.1 →	8.0.2	8.0.3	8.0.4	8.0.5	8.0.6	8.0.7	8.0.8	8.0.9	8.0.10
8.0.2 →		8.0.3	8.0.4	8.0.5	8.0.6	8.0.7	8.0.8	8.0.9	8.0.10
8.0.3 →			8.0.4	8.0.5	8.0.6	8.0.7	8.0.8	8.0.9	8.0.10
8.0.4 →				8.0.5	8.0.6	8.0.7	8.0.8	8.0.9	8.0.10
8.0.5 →					8.0.6	8.0.7	8.0.8	8.0.9	8.0.10
8.0.6 →						8.0.7	8.0.8	8.0.9	8.0.10
8.0.7 →							8.0.8	8.0.9	8.0.10
8.0.8 →								8.0.9	8.0.10
8.0.9 →									8.0.10

Compatibility Matrix for HPE Morpheus VM Essentials Software

Hardware and software is continually being tested and certified for compatibility with HPE Morpheus VM Essentials Software. For full details, see **The Compatibility Matrix for HPE Morpheus VM Essentials Software**. Items not listed in that document may be compatible but are untested.

Elevating to HPE Morpheus Enterprise

This section of the guide goes over the process for upgrading a HPE Morpheus VM Essentials Software appliance to a HPE Morpheus Enterprise Software appliance. HPE Morpheus VM Essentials and HPE Morpheus Enterprise are essentially the same product with HPE Morpheus VM Essentials focused specifically on management and consumption of HVM clusters and HPE Morpheus Enterprise adding on support for many other public and private Cloud types with a richer orchestration and automation experience (in addition to all features included with HPE Morpheus VM Essentials). HPE Morpheus Enterprise requires separate licensing, reach out to your account manager if you're unsure which licensing entitlements you can access. This guide is intended for HPE Morpheus VM Essentials administrators to upgrade their existing appliances and assumes a level of comfort with the Linux command line and the version upgrade process for HPE Morpheus VM Essentials and/or HPE Morpheus Enterprise. After upgrading, refer to HPE Morpheus Enterprise **documentation** for use guides to consuming the full HPE Morpheus Enterprise feature set.

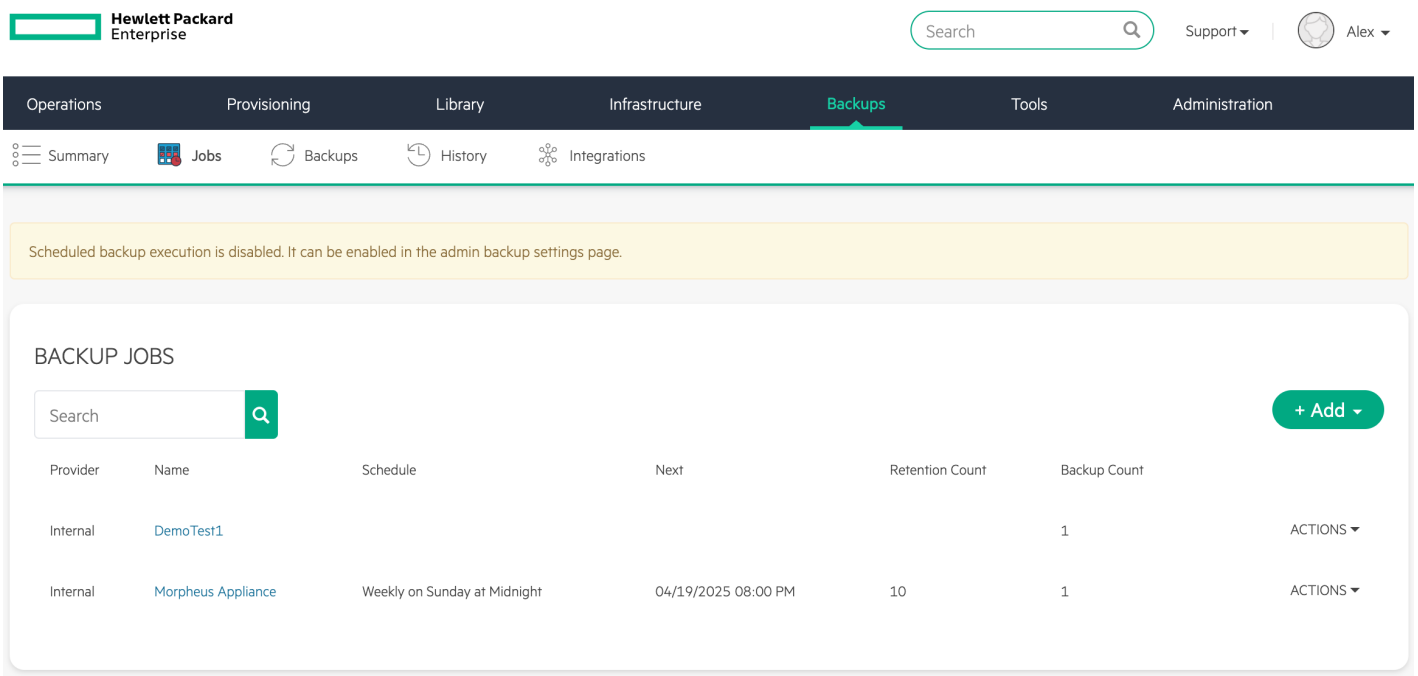
Prerequisites

- HPE Morpheus VM Essentials manager version 8.0.1+
- A bucket integrated with HPE Morpheus VM Essentials manager which can house an appliance database backup
- The HPE Morpheus Enterprise upgrade package (version 8.0.4+)
- A HPE Morpheus Enterprise license to add following the upgrade to enable the full feature set

Back Up the Appliance

Start by taking a fresh backup of the appliance database. View the appliance backup job by navigating to Backups > Jobs. As in the

screenshot, there should be a backup job named “Morpheus Appliance.” If an appliance backup job is not shown, enable the “Backup Appliance” setting within global settings (Administration > Settings > Backups).



Click Run Now and wait for a new green checkmark to appear indicating a new run of the backup job was successful.

Package Installation

Upgrading the HPE Morpheus VM Essentials manager to a HPE Morpheus Enterprise appliance is as simple as installing the HPE Morpheus Enterprise package over the existing HPE Morpheus VM Essentials package in a process very similar to version upgrades you may have done in the past. First, download the HPE Morpheus Enterprise `.deb` package. The download URL shown below is a placeholder, reach out to your account manager if you’re unsure where to find the download URL for the latest package.

```
wget https://url.to.morpheus-appliance_x.x.x-x.deb
```

Next, stop the HPE Morpheus VM Essentials UI.

```
sudo morpheus-ctl stop morpheus-ui
```

Install the HPE Morpheus Enterprise package and force it to overwrite.

```
dpkg -i --force-overwrite morpheus-appliance_x.x.x-x.deb
```

Wait for the installation to complete. There will be warnings about conflicts which may be safely ignored. When installation is complete, you will see a message similar to the screenshot below:

```
Thank you for installing Morpheus!
Configure and start the Morpheus admin web UI by running the following command:

sudo morpheus-ctl reconfigure

Morpheus should be reachable at https://vmem-01
Otherwise configure Morpheus for your system by editing /etc/morpheus/morpheus.rb file
and running reconfigure again.

WARNING! ROLLING UPGRADES FOR HA ENVIRONMENTS ONLY SUPPORTED WHEN UPGRADING FROM v7.0.3+ or v6.2.11
Performing a rolling upgrade on other versions will result in RabbitMQ deserialization errors.
Stop the morpheus-ui service on all app nodes prior to upgrading any other versions.

root@vmem-01:~#
```

Now, remove the HPE Morpheus VM Essentials package.

```
sudo apt-get remove -y hpe-vm-essentials
```

Following removal, restart any recommended services if prompted.

```
root@vmem-01:~# sudo apt-get remove -y hpe-vm-essentials
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  hpe-vm-essentials
0 upgraded, 0 newly installed, 1 to remove and 12 not upgraded.
After this operation, 2,598 MB disk space will be freed.
(Reading database ... 150374 files and directories currently installed.)
Removing hpe-vm-essentials (8.0.4-1) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.

Restarting services...
 systemctl restart morpheus-runsvdir.service

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@vmem-01:~#
```

We must now clean up OpenSearch directories. Currently, HPE Morpheus Enterprise uses ElasticSearch while HPE Morpheus VM Essentials manager uses OpenSearch. Migration through snapshots is not supported due to this incompatibility. In general, OpenSearch and ElasticSearch contain VM performance metrics. This data can be considered ephemeral and safely deleted as the default retention is only 30 days. HPE Morpheus Enterprise is planned to migrate to OpenSearch in the future and at that point, this cleanup step will not be required and metrics will persist across an upgrade to HPE Morpheus Enterprise. Remove the following directories:

```
rm -rf /var/run/morpheus/opensearch
rm -rf /opt/morpheus/service/opensearch
```

Next, run the reconfigure command. This will configure ElasticSearch for use with the upgraded appliance.

```
sudo morpheus-ctl reconfigure
```

Once the reconfigure is complete, make sure all HPE Morpheus Enterprise services are started

```
sudo morpheus-ctl status
```

If any services need started, use the following command:

```
sudo morpheus-ctl start {service name}
```

You can watch the logs to see when the UI comes back up:

```
sudo morpheus-ctl tail morpheus-ui
```

When the Morpheus ASCII logo appears, you should be able to reach the UI from a web browser.

Upgrading the License

Now that HPE Morpheus Enterprise UI is reachable, the license must be upgraded. Navigate to Administration > Settings > License where you'll see a field to paste in your license key. Once again, contact your account manager if you have questions on accessing your license key.

Finally, make sure you select the appropriate option of either stacking the license onto an existing license or replacing it. Then, click Update.

At this point, the process is complete. Now that the full Morpheus feature set is unlocked, refer to Morpheus **documentation** going forward.

Operations

Subtopics

- Dashboard
- Wiki
- Activity

Dashboard

The Dashboard is a single, high-level view into your environment which includes easy-to-read performance and configuration information. In many cases other areas within VM Essentials UI will allow you to drill deeper into the information presented in the dashboard.

Subtopics

- Environment
- System Status
- Favorites
- Instance Status
- Instances By Cloud
- Group Workloads
- Cloud Workloads
- Cluster Workloads
- Backups
- Task Executions
- Activity

Environment

- **Groups:** Total number of Groups currently created
- **Clouds:** Total number of Clouds currently integrated
- **Clusters:** Total number of clusters currently provisioned
- **Apps:** Total number of Apps currently provisioned
- **Instances:** Total number of Instances currently provisioned
- **Users:** Total number of VM Essentials user accounts

System Status

System status gives a high-level view of the health of the appliance. More detailed information can be viewed on the appliance health detail page (Administration > Health) and a more detailed breakdown of the meaning of each status indicator is in VM Essentials **health**

documentation.

Favorites

Any Instances you've "favorited" will appear here along with the Instance name, type, and IP address

Instance Status

The total number of Instances is listed along with a pie chart showing the statuses of each. Hover over each section of the pie chart to see the total number and percentage of Instances in that state. States may include running, stopped, provisioning, and more

Instances By Cloud

The total number of Clouds which currently have an Instance provisioned is shown. Hover over each section of the pie chart to see the total number and percentage of Instances provisioned to each Cloud

The number of Instances that have existed at any point in the day with additional breakdown to show the number provisioned to each Cloud. This number will include any pre-existing Instances which have carried over from previous days along with any new Instances that were provisioned and existed on that day even for a short time

Group Workloads

The instantaneous count of host or container records broken down by Group association

Cloud Workloads

The instantaneous count of host or container records broken down by Cloud association

Cluster Workloads

The instantaneous count of managed containers broken down by Cluster association

Backups

Displays the number of successful and unsuccessful backups over the last day, week or month

Task Executions

Displays the number of successful and unsuccessful Task executions over the last day, week or month

Activity

The activity list displays the last few events that have taken place in VM Essentials by any user. This could be new provisioned workloads, deleted workloads, backups, or a number of other things. A more complete list of recent activities can be viewed in Operations > Activity

Wiki

The Morpheus Wiki is a tenant-wide, RBAC-controlled, auditable Wiki that allows easy UI, API and CLI access to information, notes, configurations or any other data needed to be referenced or shared with others. Wiki pages can be created directly from the Wiki tab of the detail page for various resource types, including Clouds, Groups, Servers, Instances, and Clusters. Wiki pages created this way are automatically categorized under the appropriate resource type. Additional Wiki pages and custom categories can be created when viewing the whole Wiki at Operations > Wiki. Here you will also see the complete Wiki, including pages created on various object detail pages which are categorized appropriately.

Subtopics

- Highlights
- Creating Wikis
- Hosting Images

Highlights

- Main Wiki section is at Operations > Wiki
- Wiki tabs are on Clouds, Groups, Instances, Hosts, VMs, and Clusters detail pages
- Additional Wiki Pages and Categories can be created from Operations > Wiki
- When a Wiki tab is populated, a Page is automatically added and accessible at Operations > Wiki
- The Wiki is accessible from the UI, CLI and API.
- Wiki access is RBAC-controlled via the Operations: Wiki permission in Roles (None, Read and Full)
- Page updates are stamped with the “Last Updated By” user and the time the edit was made
- Wiki pages can be searched from `/operations/wiki` or navigated from `/operations/wiki-page/page-index`
- All wiki pages are encrypted using AES 256-bit encryption
- Wiki pages use Flexmark for Markdown. Annotate your Wiki pages with headers, text styling, code blocks, hyperlinks, and more as needed
- Create a new page with title “Home” to replace the default Wiki landing page that ships with VM Essentials

Creating Wikis

The Wiki service ties into assets throughout the environment. Create pages for Instances, hosts, groups, Clouds, and even clusters directly on their detail pages (see the Wiki tab). Users may also just create general notes pages in the centralized Wiki section (Operations > Wiki)in Markdown format.

Creating your first page is as simple as clicking the Create Page button from the Wiki home page (Operations > Wiki). Write down some content, give the page a title, and click SAVE. The Wiki will also keep track of who last edited a page and when. The beauty of this Wiki is that it's clean and easy to write down notes related to various parts of your application deployment or infrastructure without going to an external tool. Many VM Essentials constructs, such as Instances, hosts, and more, also have their own Wiki page. Navigate to the detail page for the selected construct, open the Wiki tab, and click EDIT to add content.

IMPORTANT

All wiki pages are encrypted using AES-256 bit encryption. Though we don't advise storing passwords in a Wiki document (services like Cypher are for that), role-based access control also can properly restrict access to content related to Instances or hosts which the user may not have access to.

Hosting Images

It's possible to add images to your Wiki pages and images can be sourced from the Internet, a Cloud storage bucket (like an AWS S3 Bucket), or even from files stored to the VM Essentials appliance's local file system. Within your Wiki page markdown, add your image using the following syntax:

```
![my alt text](https://myimage.com/image.jpg)
```

The text within the square brackets [] sets the HTML "alt" description for the image and the URL within parentheses () is the "src" URL for the image. The VM Essentials **Archives** feature is a great resource for hosting images for use in Wiki. Archives can target cloud storage buckets or even file shares on the VM Essentials appliance local storage. VM Essentials generates an access URL for each file stored in Archives, simply target this URL in your markdown to show an image stored in VM Essentials Archives within your Wiki pages.

Activity

The Activity section displays a recent activity report for Auditing. VM Essentials defines an activity as any major action performed on an instance or server, such as, but not limited to adding a server, deleting a server, provisioning an instance, deleting an instance, creating a backup, etc... This view can be searched and filtered by type, user, and date range.

Subtopics

Activity
History

Activity

There are four types of activities that are displayed in the Activity Reports:

- Backup
- Provisioning
- Alert

Subtopics

To View a Recent Activity report:
Review

To View a Recent Activity report:

Procedure

1. Select the `Operations` link in the navigation bar.
2. Select `Activity` in the sub navigation bar.

Results

Recent activity is displayed in order from recent to oldest. This view can be searched and filtered by type, user, and date range.

Review

To review the item that generated the activity, click the name of the activity and it will go to a new page and display that item. The list of activity can be filtered by type, user or date range.

NOTE

Deleted activities are displayed as an alert and do not contain a link to the event item. If the activity is not a deletion event we provide a link on the activity name to go to the item the activity occurred on. Delete activity alerts are shown for Instances, servers, Clouds, and Groups.

History

The HISTORY section shows process history from Instance processes. This is an aggregate view of the `History` tab contained in each Instance detail page.

Processes can be expanded to view all process steps and process history detail including output and errors.

Access to HISTORY is given by the `Operations:Activity` Role permission.

The Logs displayed in `Administration - Health - Morpheus Logs` are from `/var/log/morpheus/morpheus-ui/current`. These logs show all ui activity and are useful for troubleshooting and auditing.

NOTE

Stack traces in `Administration - Health - Morpheus Logs` are filtered for VM Essentials services. Complete stack traces can be found in `/var/log/morpheus/morpheus-ui/current`.

Provisioning

There are many capabilities in the VM Essentials provisioning engine ranging from virtual machines bound for VMware vCenter and HVM cluster targets to containerized workloads targeting Docker. Deployment management and library template construction are also core aspects of the provisioning engine. This section of VM Essentials documentation covers the provisioning engine itself while the Library section covers template building, image management, and automation stacks.

Subtopics

Requirements

Provisioning Concepts

Instances

Requirements

Provisioning Instances typically involves many steps beyond starting a workload and VM Essentials is centered around automating everything for your application to be fully operational. There is a lot that goes on when spinning up an Instance, and to make the magic happen a few requirements need to be met.

> **IMPORTANT**
> By default, Agent Installation is enabled when provisioning unless deselected on the Virtual Image or SKIP AGENT INSTALL is selected from the provisioning wizard.

Subtopics

VM Provision Steps
Virtual Images
Agent Install

VM Provision Steps

While many things can happen during an individual provisioning process, the basic order is:

- Look for the Virtual Image

  VM Essentials will check if the Virtual Image set on the Node Type or selected from a list of images during provisioning is already available to the HVM cluster or to a vCenter Cloud target. If not and it is an uploaded or local image, VM Essentials will attempt to upload the image to the HVM cluster or vCenter target.

  Upload Image

  For uploaded or local images that do not exist in the target, VM Essentials will need to upload the Image. Ensure the Virtual Image is valid for the target technology, the image meets the target upload requirements, and VM Essentials has network access and permissions to upload the image.

  > **NOTE**
  > When uploading an image to a VMware Cloud, the Virtual Image is copied directly to the target ESXi host, NOT through the vCenter server. Ensure the VM Essentials Appliance(s) can resolve target ESXi hostnames and connect on port 443 for successful vmdk/ova uploads.

  Clone Image

  Once the Image is confirmed available in the target cloud, VM Essentials will clone the Image to the target Datastore.

  > **NOTE**
  > The target host must have access to the target Datastore of the Image

- Reconfigure Image

  Once cloned, VM Essentials will resize the Image based off provisioning parameters

- Cloud-init (if enabled)

  Attached cloud-init iso

When using cloud-init, VM Essentials will attach a tiny metadata iso to the new VM. Network, Machine, User and any other cloud-init metadata will be sourced from this iso.

VM Tools

VM Essentials will run guest customizations via VMware VM Tools, including network config when assigning static IP addresses.

- Wait for Power On status and Network info

  VM Essentials will wait to hear back from the target that the VM has successfully started and has an IP address.

  > **NOTE**
  > If VM TOOLS INSTALLED? is NOT checked on the source Virtual Image configuration, VM Essentials will skip waiting for network.

- Finalize

  By default, this step will include Agent installation.

  > **IMPORTANT**
  > If the VM is stuck in finalize for long periods of time, this typically means the Agent cannot be installed or has not been heard back from. This will result in a ! warning Instance status upon provisioning completion.

  If agent installation is not possible or is not desired, uncheck “Install Agent” on the source Virtual Image configuration or select “Skip Agent Install” during provisioning to speed up provisioning completion.

Virtual Images

The most common provisioning method within VM Essentials involves Virtual Machines, and the most important part of provisioning a VM is the Virtual Image. When provisioning a VM, VM Essentials will need to do a few things depending on the location of the Virtual Image and if agent install and console access are desired.

Synced Images need to be properly configured

VM Essentials gathers as much metadata for synced images as possible, but depending on the target (HVM cluster or VMware vCenter), OS, image configuration, or agent install settings, the synced Virtual Images may not be ready to provision without some configuration within VM Essentials. The Virtual Image is already at the target Cloud, but datastore selection, credentials, cloud-init settings, networks, and security settings on the Virtual Image can cause provisioning issues.

Local/Uploaded Virtual Images

Images uploaded to VM Essentials are configured during the Add Virtual Image process, however VM Essentials in most scenarios will still need to copy the Virtual Image to the target Hypervisor/Cloud upon the first provision to the target Cloud. In addition to the requirements for provisioning a synced Virtual Image, copying an uploaded Virtual Image to the target Cloud is required. Network and image configurations can cause upload failures, resulting in provisioning issues.

Subtopics

Synced Images
Local Virtual Images

Synced Images

When a provisioning target (Cloud) is added, all available image and template records from that Cloud will be synced in regardless of Inventory settings on the Cloud. These image records will be available in the Virtual Images section and can be provisioned by using the

target clouds generic Instance Type (ex. By selecting the HVM or VMware Instance Type from the provisioning wizard).

> **NOTE**
>
> Synced Virtual Images are just metadata records in VM Essentials pointing to the image in the target Cloud. The actual image files are not copied/imported to VM Essentials manager.

Before provisioning a synced Virtual Image, ensure the image is configured properly:

Name

Name of the Virtual Image in VM Essentials. This can be changed from the name of the image, but editing will not change the name of the actual image file.

Operating System

Specifies the platform and OS of the image. All Windows images will need to have Operating System specified on the Virtual Image, as VM Essentials will assign Linux as the platform for all images without an operating system specified.

Minimum Memory

The Minimum Memory setting will filter available Plan options during provisioning. Plans that do not meet the minimum memory value set on the Virtual Image will not be provided as Plan choices by the provisioning wizard.

Cloud Init Enabled?

On by default, uncheck for any image that does not have Cloud-Init or Cloudbase-Init installed.

> **IMPORTANT**
>
> Provisioning a Virtual Image that has Cloud Init Enabled? checked on the Virtual Record in VM Essentials but does not have cloud-init installed will result in immediate provisioning failure.

Install Agent

On by default, uncheck to skip Agent install. Note this will result in the loss of utilization statistics, logs, Task execution, and monitoring (Some utilization stats are still collected by Agent-less workloads).

Username

An existing Username on the Image. This is required for authentication, unless VM Essentials is able to add user data, Cloud-Init, Cloudbase-Init or Guest Customizations. If Cloud-Init, Cloudbase-Init Guest Customizations or Nutanix Sysprep are used, credentials are defined in Administration > Settings > Provisioning and User Settings. If credentials are defined on the Image and Cloud-Init is enabled, VM Essentials will add that user during provisioning, so ensure that user does not already exist in the image (aka `root`). For Windows Guest Customizations, VM Essentials will set the Administrator password to what is defined on the image if Administrator user is defined. Do not define any other user than Administrator for Windows Images unless using Cloudbase-init. VM Essentials recommends running Guest Customizations for all Windows Images, which is required when joining Domains as the SID will change.

Password

Password for the existing user on the image if the Username field is populated.

Storage Provider

Location where the Virtual Image will be stored. Default Virtual Image Storage location is `/var/opt/morpheus/morpheus-ui/VMs`. Additional storage providers can be configured in Infrastructure > Storage.

Cloud-Init User Data

Accepts what would go in `runcmd` and can assume bash syntax. Example use: Script to configure satellite registration at provision time.

Auto Join Domain?

Enable to have Instances provisioned with this image auto-join configured domains (Windows only, domain controller must be configured in Infrastructure > Network and the configured domain set on the provisioned to Cloud or Network).

VirtIO Drivers Loaded?

Enable if VirtIO Drivers are installed on the image for provisioning to KVM-based hypervisors, such as HVM cluster

VM Tools Installed?

On by default, uncheck if VMware Tools (including OpenVMTools) are not installed on the Virtual Image. VM Essentials will skip

network wait during provisioning when deselected.

Force Guest Customization?

VMware only, forces guest customizations to run during provisioning, typically when provisioning to a DHCP network where guest customizations would not run by default. This is required for host/computer name definitions. domain joining, licenses and user definitions when using DHCP.

Trial Version

Enable to automatically re-arm the expiration on Windows Trial Images during provisioning.

IMPORTANT

Provisioning a Virtual Image that has Cloud Init Enabled? checked on the Virtual Record in VM Essentials but does not have cloud-init installed will result in immediate provisioning failure.

IMPORTANT

For Linux images without cloud-init, an existing username and password must be defined on the Virtual Image record for Agent Install, Domain joining, licensing, script execution and other automation, and SSH or RDP Console access.

Local Virtual Images

A Local Virtual Image means it has been uploaded to VM Essentials. To provision, VM Essentials will need to upload the image to the provisioning target upon first provision.

- Ensure the Virtual Image is valid for the target Cloud, the Image meets the target cloud upload requirements, and VM Essentials has network access and permissions to upload the image.

NOTE

When uploading an image to a VMware Cloud, the Virtual Image is copied directly to the target ESXi host, NOT through the vCenter server. Ensure the VM Essentials Appliance(s) can resolve target ESXi hostnames and connect on port 443 for successful vmdk/ova uploads.

Once a local Virtual Image has been uploaded to a provisioning target, subsequent provisions will use the image local to the target instead of uploading again as long as the copied image is still available.

Agent Install

When provisioning an Instance, there are some network and configuration requirements to successfully install the Agent. Typically when a VM Instance is still in the provisioning phase long after the VM is up, the Instance is unable to reach VM Essentials, or depending on Agent install mode, VM Essentials is unable to reach the Instance.

The most common reason an Agent install fails is the provisioned Instance cannot reach the VM Essentials Appliance via the `appliance_url` set in Administration > Settings over both 443 and 80. When an Instance is provisioned from VM Essentials, it must be able to reach the VM Essentials appliance via the `appliance_url` or the Agent will not be installed.

In addition to the main `appliance_url` in Administration > Settings, additional `appliance_urls` can be set per Cloud in the Advanced options of the Cloud configuration pane when creating or editing a Cloud. When this field is populated, it will override the main appliance URL for anything provisioned into that Cloud.

TIP

The VM Essentials current log, located at `/var/log/morpheus/morpheus-ui/current`, is very helpful when troubleshooting Agent installations.

Subtopics

Agent Install Modes
SSH/Winrm
VMware tools (vmtools) RPC mode
Cloud-Init Agent install mode

Agent Install Modes

There are 3 Agent install modes:

- SSH/WinRM
- VMware Tools
- Cloud-init

Subtopics

For All Agent Install modes

For All Agent Install modes

When an Instance is provisioned and the Agent does not install, verify the following for any agent install mode:

- The VM Essentials `appliance_url` (Administration > Settings) is both reachable and resolvable from the provisioned node.
- The `appliance_url` begins with to `https://`, not `http://`.

> **NOTE**
> Be sure to use `https://` even when using an IP address for the appliance.

- Inbound connectivity access to the VM Essentials Appliance from provisioned VMs and HVM cluster hosts on port 443 (needed for Agent communication)
- Private images (those not provided with VM Essentials by default) must have their credentials entered. These can be entered or edited in the Library > Virtual Images section by clicking the edit button (pencil icon) next to the appropriate image.

> **NOTE**
> Administrator user is required for Windows agent install.

- The Instance does not have an IP address assigned. For scenarios without a DHCP server, static IP information must be entered by selecting the Network Type: Static in the Advanced section during provisioning. IP Pools can also be created in the Infrastructure > Network > IP Pools section and added any Cloud's network section for IPAM.
- DNS is not configured and the node cannot resolve the appliance. If DNS cannot be configured, the IP address of the VM Essentials appliance can be used.

SSH/Winrm

Subtopics

Linux Agent
Windows Agent

Linux Agent

- Port 22 is open for Linux images, and SSH is enabled
- Credentials have been entered on the image if using a custom or synced image. Credentials can be entered on images in the Library > Virtual Images section.

Windows Agent

- Port 5985 must be open and WinRM enabled for Windows images.
- Credentials have been entered on the image if using custom or synced image. Credentials can be entered on images in the Library > Virtual Images section.

NOTE
Administrator user is required for Windows agent install.

VMware tools (vmtools) RPC mode

- VMware tools is installed on the template(s)
- Credentials have been entered on the Image if using an uploaded or synced image when Cloud-init or Guest Customizations or Sysprep for Windows are not used. Credentials can be entered on Images in the Library > Virtual Images section.

Cloud-Init Agent install mode

- Cloud-Init is configured in Administration > Settings > Provisioning section
- Provisioned image has Cloud-Init (Linux) or Cloudbase-Init (Windows) installed

Provisioning Concepts

VM Essentials is a powerful provisioning and management platform for HVM clusters and VMware vCenter private cloud. Compared to other CMP platforms in the space, some terminology and concepts may differ. These concepts are documented in this section along with places where terminology may be slightly different compared with other platforms or with common industry parlance.

Subtopics

Instances
Containers / Nodes / Virtual Machines
Hosts / Servers

Instances

VM Essentials starts with provisioning Instances. In some platforms, an Instance is representative of a singular object like a virtual machine in VMware vCenter. In VM Essentials, this concept was rethought. An Instance is more of a representation of a resource or service. This service may involve several virtual machines, as in the case of a database cluster or horizontally-scaled web servers.

When viewing an Instance detail page, one is able to look at details and statistics specific to a virtual machine or container. VM Essentials simply helps simplify the management model for tracking these services.

Containers / Nodes / Virtual Machines

In relation to Instances, an Instance can have many nodes. A node is a generic representation of a container or a virtual machine. In most cases, VM Essentials will represent a node as a Container or Virtual Machine depending on the provisioning engine used for the Instance (workload provisioned to a HVM cluster as opposed to a Docker cluster, for example). Node is just a generic naming representation when referring to these types of items. The public VM Essentials developer API, however, often refers to both virtual machines and Docker containers as “containers”. The UI was updated to better delineate this concept for easier understanding but, in essence, the name is valid for both concepts of containerized environments as well as virtual machines.

Hosts / Servers

This concept is mostly tailored to users of VM Essentials who are responsible for managing and maintaining the underlying infrastructure integrations. A Host typically refers to a Docker Host in which a container (within an Instance) is running, or a hypervisor that virtual machines can be provisioned onto. A server is the underlying general representation of a physical or virtual server. It could be a Host representation, a Virtual Machine, or even a Bare Metal delineation.

When a user provisions a VM-based Instance, a corresponding server record is created to represent the link to the actual resource via the underlying provisioning engine. This may seem a bit odd but provides an aspect of VM Essentials that is quite powerful. This singular concept is what allows VM Essentials to ingest “brownfield” environments. We do not need to start clean. VM Essentials can be integrated into existing environments and manage existing virtual machines. The way VM Essentials does this is by periodically syncing existing VMs from the added cloud integrations. A server record will be created and periodically updated (every five minutes, by default) with realtime information and changes. This, in essence, provides CMDB-like capabilities as well. When a server is discovered, the user (given the appropriate access) can convert the virtual machine to a managed Instance. When this is done, a corresponding Instance is made in the provisioning section of VM Essentials and the VM Essentials Agent can optionally be installed to provide more refined guest operating system-level statistics and logging.

Instances

Instances are a great starting point for taking advantage of self-service features and spinning up both VMs and containers. The top of the main Instances page shows overall statistics for the listed Instances, including count, status, and resource utilization. You can search for Instances by name, or filter by group, type, or category.

The Instance list contains important information about each Instance, including the Instance name, environment tag, type, IP address and port info, Instance version, the number of virtual machines or containers, the Group, and the associated Cloud.

Subtopics

- Creating Instances
- Managing Instances

Creating Instances

Creating Instances

The Instance catalog is where you will create new workloads targeting the HVM clusters and/or VMware vCenter Clouds available to the VM Essentials environment. The list contains only Instance Types relevant to the provisioning engines which enabled and integrated in the current appliance.

To get started, simply click the + Add button in the upper right of the Provisioning > Instances page. A modal will display allowing the catalog to be searched. Once an item is selected, it is just a matter of following the steps through the wizard.

TIP

The Instance catalog can be customized via role-based access control (RBAC) to restrict provision types only to certain Roles. It is completely customizable.

The next step will ask for a Group and Cloud to be selected. The Group is an abstract representation that can contain multiple HVM clusters or VMware vCenter integrations. Clouds can be in multiple Groups and Groups are also useful for using RBAC to restrict provisioning access and set retainment policies. The wizard continues by allowing us to choose a name for the Instance as well as an environment.

NOTE

Currently the Environment option is most useful for presenting the user with informative metadata around the Instance when coming back to it later.

Moving on, it is now time to configure the Instance. Depending on the Instance Configuration that is chosen, fields will change. This can include cloud-specific fields (i.e. target hosts for HVM clusters or datastores for VMware Clouds). There will also be options like setting an initial user account. Some of these fields are optional and will be represented as such in the wizard.

One last step before the Instance can be provisioned is the Automation step. It is here that you can select Tasks which will run during the provision process and these Tasks must complete successfully in order for the Instance status to be reported as successful. Tasks are either Bash or Powershell scripts which can be configured in the Library > Automationsection.

Now that the steps are completed for provisioning the selected Instance type, simply review your selections and complete. The Instance will automatically show up in the Instances list and its provisioning state will be represented. Depending on what was provisioned this step can range from seconds to minutes.

Subtopics

- Converting Discovered Resources to Managed Instances

Converting Discovered Resources to Managed Instances

When creating new cloud integrations (or updating existing ones), users may opt for VM Essentials to onboard any existing resources that currently reside in the Cloud. For example, these may be virtual machines that exist on vCenter hosts prior to integration with VM Essentials. With the Add/Edit Cloud modal open, mark INVENTORY EXISTING INSTANCES for VM Essentials to automatically onboard these resources. Not only will VM Essentials inventory these hosts at the time the cloud is integrated (or updated), it will also continue to poll the target cloud every five minutes (by default) for newly added or removed servers. Users can see these discovered servers by looking in Infrastructure > Compute. Depending on the type of resource, it may appear on the Virtual Machines tab, the Containers tab, or another tab. Additionally, we can see a list of discovered servers on Cloud detail pages (Infrastructure > Clouds > Selected Cloud). Just click on the tabs for VMs, Containers or Hosts tab. Discovered resources will be indicated as such whereas containers which are associated with a managed Instance will be marked as a “Managed”.

Additionally, VM Essentials allows users to convert discovered resources into managed Instances. Begin from the server detail page (Infrastructure > Compute > Virtual Machines > selected machine) and from the ACTIONS menu select “Convert to Managed”. At this point, we must make a number of selections:

- Select a Group (this dropdown contains a filtered list of Groups in which the associated Cloud resides)
- Username and password for a seeded account
- Opt to install VM Essentials Agent or not
- Select the Instance Type which should be associated with the new Instance containing this VM
- Identify the operating system
- Select a Plan (this dropdown contains a filtered list of plans which correlate to the size of the VM)

Finally, click EXECUTE. Once this process is completed, the server will be indicated as “Managed” in the servers list. Additionally, a new Instance will appear on the Instances List page (Provisioning > Instances). We can now work with it in the same way we can work with any other Instance, such as by expanding the Instance horizontally with added nodes.

Managing Instances

Instance actions allow you to perform numerous management tasks on instances. The actions available depend on the instance type, hypervisor, roles permissions, and instance state. Actions can be accessed from the Instances list page or from an Instance detail page.

Edit

Edit the Name, Description, Environment, Group, Tags, and Owner for the Instance.

Delete

Deletes the Instance.

IMPORTANT

Deleting an Instance will delete the actual underlying VMs or Containers and cannot be undone.

TIP

You can change the owner of an instance easily by selecting the edit button and entering a new owner in the corresponding field.

Subtopics

Actions
Performing Instance Actions
Notes

Actions

Available options in the Actions dropdown can include:

Suspend

Puts the VM in a suspended state without shutting down the OS.

Stop/Start/Restart Server

Stops, Starts or Restarts the Virtual Machine.

Import as Image

Clones and exports VM in its current state to target Storage provider and adds a Virtual Image record with metadata matching the source Instance configuration.

Clone to Image

Clones and converts VM in its current state to image in the source Cloud and adds a Virtual Image record with metadata matching the source Instance configuration.

Lock/Unlock Instance

A locked Instance cannot be deleted until it is unlocked.

Reconfigure

The Reconfigure action allows service plan, disk, CPU, memory, networks and storage controller changes. Available options depend on the type and Plan configuration. Some resize actions require an Instance restart.

Clone

Creates a new Instance from the Instance at its current state.

Backup

Immediately executes a backup of the Instance. This is only available for Instances with backups enabled.

Run Task

Select a currently-configured Task to run against the Instance. Tasks can be created and edited in Library > Automation.

Add Node

Adds an additional node to the configuration. Additional options and configurations are required in the add node wizard depending on Instance configuration and type.

Eject Disk

Ejects attached disks (ISOs).

Clone to Template (VMware)

Creates a new VMware Template from the Instance with corresponding VM Essentials Virtual Image record.

TIP

Scrolling down in the Actions dropdown may be necessary to see all options.

Performing Instance Actions

Procedure

1. Select the Provisioning link in the navigation bar.
2. From the Instances list, select the desired Instance.
3. Click the Actions dropdown button and select an Action.

Notes

Every Instance has a Wiki section for adding useful information about the Instance. Wiki can be added by selecting the Wiki tab on the bottom of the Instance Detail page. Instances with associated VMware VMs will bi-directionally sync VM Essentials Wiki content and VMware VM Notes. See the Wiki Section for more details.

TIP

Markdown Syntax is supported in Wikis.

Library

Subtopics

- Labels
- Automation
- Virtual Images

Labels

Labels are a categorization feature designed to allow easier filtering of list views in the VM Essentials Library. The following library constructs can be labeled:

- Clouds
- Groups
- Tasks
- Instances
- Servers
- Virtual Images

Labels are visible from the list views of any constructs listed above. By default, labels are turned on in the list view but if they aren't showing, click the gear icon (⚙) and then click Labels to enable them.

The list view contains a row of filters above the list, one of which is Labels. Enter a search string to find an existing label or click the dropdown button within the field to select an existing label. This will filter the list to show only constructs which have the selected label.

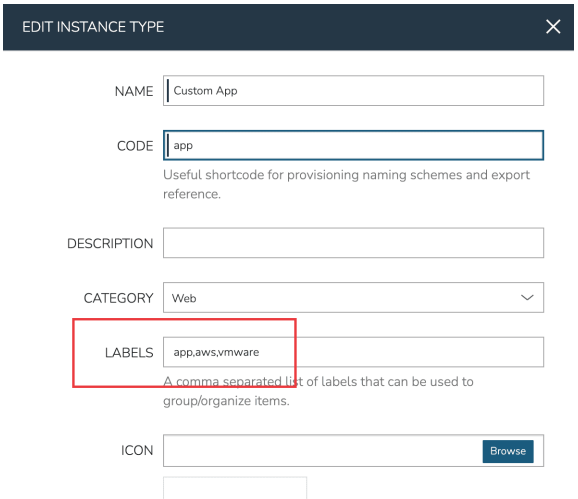
> **NOTE**
> Any list may be filtered by any label which exists on any construct. When a label is removed from a construct and no other constructs also have that label, VM Essentials will remove the label from the list during its nightly sync. It is normal for a label to continue to exist in this list, even if it's not currently applied to any constructs, until the next nightly sync has taken place.

Subtopics

Adding and Removing Labels
Running Automation Against Label Targets

Adding and Removing Labels

Labels can be created when adding or edited any of the supported constructs listed above. When adding or editing the object, enter or edit the comma-separated list of labels you wish to apply.



Running Automation Against Label Targets

Tasks can be run against Instance Labels or Server Labels. When executing the Task, select either Server Label or Instance Label. After specifying the Label, the automation will be run against all Instances or Servers which have the indicated Label. Currently, only one Label may be selected and users cannot enter multiple Labels in the field. If a non-existent Label is entered, the automation simply will not run against any Workloads since the Label does not match any.

NOTE

Instance and server Labels are separate. Even if some Instances or servers have the same Label, the automation is only run against the selected construct (Instance Labels or Server Labels).

Automation

Library > Automation

The automation section is where scripts, known as Tasks, can be created. Tasks are individual Bash or Powershell scripts which can be selected to run against Instances at the time they are provisioned from the Instance provisioning wizard. In this section, users can also create execution schedules which are configured time intervals on which automated jobs (such as backups) would be carried out.

Subtopics

- Tasks
- Execute Scheduling

Tasks

Subtopics

- Role Permissions
- Target Options
- Execute Options
- Source Options
- Allow Custom Config
- Adding Tasks
- Editing Tasks
- Deleting Tasks

Role Permissions

The User Role Permission 'Provisioning: Tasks FULL' is required to create, edit and delete Tasks.

Subtopics

- Common Options

Common Options

When creating a Task, the required and optional inputs will vary significantly by the Task type. However, there are options which are common to Tasks of all types.

Target Options

When creating a Task, users can select a target to perform the execution. Some Task types allow for any of the three execution targets listed below and some will limit the user to two or just one. The table in the next section lists the available execution targets for each Task type.

- **Resource:** A VM Essentials-managed Instance or server is selected to execute the Task
- **Local:** The Task is executed by the VM Essentials appliance node
- **Remote:** The user specifies a remote box which will execute the Task

Execute Options

- **Continue on Error:** When marked, automation stacks including this Task can continue when this Task fails. Additionally, Instances provisioned with this Task as part of its automation stack can be considered provisioned successfully even if this Task has failed
- **Retryable:** When marked, this Task can be configured to be retried in the event of failure
- **Retry Count:** The maximum number of times the Task will be retried when there is a failure
- **Retry Delay:** The length of time (in seconds) VM Essentials will wait to retry the Task
- **Allow Custom Config:** When marked, a text area is provided at Task execution time to allow the user to pass extra variables or specify extra configuration. See the next section for an example.

Source Options

Task configuration code may be entered locally or sourced via URL. Changing the SOURCE type will often update the available fields in the Task modal to accommodate the selected sourcing.

- **Local:** The Task configuration code is written directly in VM Essentials in a large text area. VM Essentials includes syntax highlighting for easier debugging and script writing
- **URL:** For Task configuration that can be source via an outside URL, specify the address in the URL field

Allow Custom Config

When “Allow Custom Config” is marked on a Task, the user is shown a text area for custom configuration when the Task is executed manually from the Tasks List Page. This text area is inside the “Advanced Options” section, which must be expanded in order to reveal the text area. Within the text area, add a JSON map of key-value pairs which can be resolved within your automation scripts. This could be used to pass extra variables that aren’t always needed in the script or for specifying extra configuration.

Subtopics

Example JSON Map:
Task Types
Task Management

Example JSON Map:

```
{"key1": "value1",
"key2": "value2",
"os": "linux",
"foo": "bar"}
```

When the Task is executed, these extra variables would be resolved where called into the script such as in the following simple BASH script example:

```
echo "<%=customOptions.os%>"
echo "<%=customOptions.foo%>"
```

The above example would result in the following output:

```
linux
bar
```

Task Types

Available Task Types

	Task Type	Task Description	Source Options	Execute Target Options	Configuration Requirements	Role Permissions Requirements
	PowerShell Script	Execute PowerShell Script on the Target Resource	Local, Repository, Url	Remote, Resource, Local	None	Library: Tasks
	Restart	Restarts target VM/Host/Container and confirms startup status before executing next task in Workflow	System	Resource	None	Library: Tasks
	Shell Script	Executes Bash script on the target resource	Local, Repository, Url	Local, Remote, Resource	None	Library: Tasks

Task Management

Adding Tasks

Procedure

1. Select Automation from within the Library menu
2. On the Tasks tab, click the Add button
3. From the New Task Wizard input a name for the task
4. Select the type of task from from the type dropdown
5. Input the appropriate configuration details. These will vary based on the selected Task type.
6. Once done, click SAVE CHANGES

Results

TIP

When writing a Task config, it's often necessary to reference VM Essentials variables which pertain to the specific Instance the Task is being run against. VM Essentials includes a pop-out column along the right side of the Add/Edit Task modal which lists available variables. Click and drag the relevant variable into the config area and VM Essentials will automatically fill in the variable call formatted for the currently chosen Task type. See the screenshot below.

TIP

When writing a Task that calls back into the HPE Morpheus VM Essentials API, pass an `Authorization : Execution <%=executionLeaseToken%>` header. The system API will authenticate against that during the life of the Task execution only. This is preferred over other methods of authorizing Task calls as there was a risk of the token expiring in the middle of the Task run.

Editing Tasks

Procedure

1. Select Automation from within the Library menu
2. Click the pencil icon (✎) on the row of the task you wish to edit
3. Modify Task as needed
4. Once done, click SAVE CHANGES

Deleting Tasks

Procedure

1. Select Automation from within the Library menu
2. Click the trash icon ( ) on the row of the Task you wish to delete

Execute Scheduling

Execute Scheduling creates time schedules for automated jobs, such as backups. Backup Jobs are discussed in greater detail in the Backups section and are configured with an execution schedule to coordinate their run times. This section goes through the process of creating and configuring the scheduling object.

Schedules use CRON expressions, such as `0 23 * * 2` equalling `Executes every week on Tuesday at 23:00`. CRON expressions can easily be created by clicking the corresponding translation in the create or edit Execution Schedule modal below the Schedule field and selecting a new value.

NOTE

Execute Schedules CRON expressions should not include seconds or years. The days of the week should be numbered 1-7, beginning with Monday and ending with Sunday. SUN-SAT notation may also be used. For more on writing CRON expressions, many guides are hosted on the Internet including **this one**. VM Essentials execution schedules support most cron syntax but certain more complex expressions may fail to evaluate and the execute schedule will not save. Additionally, some complex expressions may save and work correctly while the friendly written evaluation below the SCHEDULE field is not interpreted correctly. This is due to an issue with the underlying library used to build this feature and cannot easily be resolved at this time.

NAME

Name of the Execution Schedule

NOTE

When assigning Execution Schedules, the name value will appear in the selection drop-down. Using a name that makes clear the time interval is often helpful.

DESCRIPTION

Description of the Execution Schedule for reference in the Execution Schedules list

TIME ZONE

The time zone for execution

Enabled

Check to enable the schedule. Uncheck to disable all associated executions and remove the schedule as an option for Jobs in the future

SCHEDULE

Enter CRON expression for the Execution Schedule, for example `0 0 * * *` equals `Every day at 00:00`

SCHEDULE TRANSLATION

The entered CRON schedule is translated below the SCHEDULE field. Highlighted values can be updated by selecting the value, and relevant options will be presented. The CRON expression will automatically be updated

Virtual Images

Subtopics

- Overview
- Configuring Virtual Images
- Provisioning Images
- Add Virtual Image

Overview

The Virtual Image section displays a list of all images, local and synced, that are available to deploy. VM Essentials includes a rich catalog of pre-configured default images for HVM clusters or for VMware vCenter Cloud targets as well. User Images are automatically synced from Cloud Integrations and added to the Virtual Images section. Images can also be uploaded directly into VM Essentials via local file or url. Understanding the process of prepping images for consumption in VM Essentials is a very important step toward building an effective VM Essentials environment.

IMPORTANT

Invalid Image Settings cause provisioning failures. VM Essentials syncs in as much metadata as possible for synced images, but additional configuration may be needed to ensure successful provisioning.

WARNING

Cloud-init is enabled by default for all Linux images. If your Linux image does not have Cloud-init installed, Cloud-init Enabled must be unchecked before provisioning the image or it will fail immediately.

Configuring Virtual Images

Subtopics

User Images

User Images

Typically VM Essentials does not have sufficient metatdata to successfully provision synced User Images with no additional configuration. After integrating Clouds and User Images have synced, it is highly recommended to configure the images prior to provisioning.

Subtopics

To edit and configure an existing Virtual Image:

To edit and configure an existing Virtual Image:

Procedure

1. Select the pencil icon at the right of any row on the Virtual Images list page, or click EDIT on a Virtual Image detail page.
2. Configure the following on the Image:

Name

Name of the Virtual Image in VM Essentials. This can be changed from the name of the image, but editing will not change the name of the actual image

Operating System

Specifies the platform and OS of the image. All Windows images will need to have the operating system specified on the Virtual Image, as VM Essentials will assign Linux as the platform for all images without an operating system specified

Minimum Memory

The Minimum Memory setting will filter available Service Plan options during provisioning. Service Plans that do not meet the minimum value set on the Virtual Image will not be provided as Service Plan choices

Cloud Init Enabled?

On by default, uncheck for any Image that does not have Cloud-Init or Cloudbase-Init installed

Install Agent?

On by default, uncheck to skip Agent install. Note this will result in the loss of utilization statistics, logs, script execution, and

monitoring. (Some utilization stats are still collected for Agent-less hosts and VMs depending on the cloud)

Username

Existing username on the image. This is required for authentication, unless VM Essentials is able to add user data, Cloud-Init, Cloudbase-Init or Guest Customizations. If Cloud-Init, Cloudbase-Init or Guest Customizations are used, credentials are defined in Administration > Settings > Provisioning and User Settings. If credentials are defined on the image and Cloud-Init is enabled, VM Essentials will add that user during provisioning, so ensure that user does not already exist on the image (such as `root`). For Windows Guest Customizations, VM Essentials will set the Administrator password to what is defined on the image if Administrator user is defined. Do not define any other user than Administrator for Windows Images unless using Cloudbase-init. VM Essentials recommends running Guest Customizations for all Windows Images, which is required when joining Domains as the SID will change

Password

Password for the user on the image if username is populated

Bucket

Location where the Virtual Image will be stored. Default Virtual Image Storage location is `/var/opt/morpheus/morpheus-ui/vms`. Additional Storage Providers can be configured in Infrastructure > Storage

Cloud-Init User Data

Accepts what would go in `runcmd` and can assume Bash syntax. Example use: Script to configure satellite registration at provision time

Create Image ID

Select FILE to browse locally for an image or drop an image file into the dropzone. Alternatively, select URL to download the image from an accessible URL. It is recommend to configure the rest of the settings below prior to uploading the source Image File(s)

Permissions

Set Tenant permissions in a multi-tenant VM Essentials environment. Select private visibility and select specific Tenants to which the Virtual Image will be made available. Select public visibility to share the Virtual Image with all Tenants

Auto Join Domain?

Enable to have Instances provisioned with this image auto-join configured domains (Windows only, domain controller must be configured in Infrastructure > Network and the configured domain set on the provisioned to Cloud or Network)

VirtIO Drivers Loaded?

Enable if VirtIO Drivers are installed on the image for provisioning to KVM-based hypervisors

FIPS Compliant Image?

When selected, VM Essentials will install the FIPS-compliant VM Essentials Agent package

VM Tools Installed?

On by default, uncheck if VMware Tools (including OpenVMTools) are not installed on the Virtual Image. VM Essentials will skip network wait during provisioning when deselected

Force Guest Customization?

VMware only, forces guest customizations to run during provisioning, typically when provisioning to a DHCP network where guest customizations would not run by default. This options requires that VMware Tools is installed on the image

Trial Version

Enable to automatically re-arm the expiration on Windows Trial Images during provisioning

Enabled Sysprep?

Applicable to VMware vCenter Clouds. Enable if the Windows Image has been sysprepped. If enabled, VM Essentials will inject `unattend.xml`

3. Click Save Changes

> **NOTE**
>
> Cloud-Init is enabled by default on all images. Images without Cloud-Init or Cloudbase-Init installed must have the `cloud-init` flag disabled on the Virtual Image setting or Provisioning may fail.

> **IMPORTANT**
>
> VM Essentials does not validate or restrict image uploads to certain file types and any type of file may be uploaded as a Virtual Image. For security purposes, these files are stored in a non-executable state so users need not worry about potentially dangerous file types being uploaded (ex. executables).

Provisioning Images

When provisioning a system image, VM Essentials will stream the image from Amazon S3 to the target Cloud if the image is not local to the Cloud.

When using images that already exist in the destination Cloud, such as synced or previously copied images, no image stream from S3 through the VM Essentials Appliance to the destination cloud will take place.

> **NOTE**
>
> The VM Essentials Appliance must be able to download from Amazon S3 when provisioning system images.

> **NOTE**
>
> The VM Essentials Appliance must be able reach and resolve the destination Host when provisioning System Images or uploaded Images for the first time. This included being able to resolve ESXi host names in VMware vCenter clouds, and reach the destination ESXi host over port 443.

Add Virtual Image

About this task

Virtual Images can be uploaded to VM Essentials from local files or URLs.

> **WARNING**
>
> Be conscious of your Storage Provider selection. The default Storage Provider is the VM Essentials Appliance at `/var/opt/morpheus/morpheus-ui/vms`. Uploading large images to the VM Essentials Appliance when there is inadequate space will cause upload failures and impact Appliance functionality. Ensure there is adequate space on your selected Storage Provider. Additional Storage Provider can be added at Infrastructure > Storage, which can be configured as the default Virtual Image Store or selected when uploading Images.

> **NOTE**
>
> VMware-type OVF Virtual Images do not support mounted ISO uploads

To Add Virtual Image:

Procedure

1. Select + Add in the Virtual Images page.
2. Select Image format:
   - ISO
   - QCOW2
   - RAW
   - VMware (vmdk/ovf/ova)
3. Configure the following on the Virtual Image:

   Name

   Name of the Virtual Image in VM Essentials. This can be changed from the name of the image, but editing will not change the name of the actual image

   Operating System

   Specifies the platform and OS of the image. All Windows images will need to have the operating system specified on the Virtual Image, as VM Essentials will assign Linux as the platform for all images without an operating system specified

   Minimum Memory

   The Minimum Memory setting will filter available Service Plan options during provisioning. Service Plans that do not meet the minimum value set on the Virtual Image will not be provided as Service Plan choices

   Cloud Init Enabled?

   On by default, uncheck for any Image that does not have Cloud-Init or Cloudbase-Init installed

   Install Agent?

   On by default, uncheck to skip Agent install. Note this will result in the loss of utilization statistics, logs, script execution, and monitoring. (Some utilization stats are still collected for Agent-less hosts and VMs depending on the cloud)

   Username

   Existing username on the image. This is required for authentication, unless VM Essentials is able to add user data, Cloud-Init, Cloudbase-Init or Guest Customizations. If Cloud-Init, Cloudbase-Init or Guest Customizations are used, credentials are defined in Administration > Settings > Provisioning and User Settings. If credentials are defined on the image and Cloud-Init is enabled, VM Essentials will add that user during provisioning, so ensure that user does not already exist on the image (such as `root`). For Windows Guest Customizations, VM Essentials will set the Administrator password to what is defined on the image if Administrator user is defined. Do not define any other user than Administrator for Windows Images unless using Cloudbase-init. VM Essentials recommends running Guest Customizations for all Windows Images, which is required when joining Domains as the SID will change

   Password

   Password for the user on the image if username is populated

   Bucket

   Location where the Virtual Image will be stored. Default Virtual Image Storage location is `/var/opt/morpheus/morpheus-ui/vms`. Additional Storage Providers can be configured in Infrastructure > Storage

   Cloud-Init User Data

   Accepts what would go in `runcmd` and can assume Bash syntax. Example use: Script to configure satellite registration at provision time

Create Image ID

Select FILE to browse locally for an image or drop an image file into the dropzone. Alternatively, select URL to download the image from an accessible URL. It is recommend to configure the rest of the settings below prior to uploading the source Image File(s)

Permissions

Set Tenant permissions in a multi-tenant VM Essentials environment. Select private visibility and select specific Tenants to which the Virtual Image will be made available. Select public visibility to share the Virtual Image with all Tenants

Auto Join Domain?

Enable to have Instances provisioned with this image auto-join configured domains (Windows only, domain controller must be configured in Infrastructure > Network and the configured domain set on the provisioned to Cloud or Network)

VirtIO Drivers Loaded?

Enable if VirtIO Drivers are installed on the image for provisioning to KVM-based hypervisors

FIPS Compliant Image?

When selected, VM Essentials will install the FIPS-compliant VM Essentials Agent package

VM Tools Installed?

On by default, uncheck if VMware Tools (including OpenVMTools) are not installed on the Virtual Image. VM Essentials will skip network wait during provisioning when deselected

Force Guest Customization?

VMware only, forces guest customizations to run during provisioning, typically when provisioning to a DHCP network where guest customizations would not run by default. This options requires that VMware Tools is installed on the image

Trial Version

Enable to automatically re-arm the expiration on Windows Trial Images during provisioning

Enabled Sysprep?

Applicable to VMware vCenter Clouds. Enable if the Windows Image has been sysprepped. If enabled, VM Essentials will inject `unattend.xml`

NOTE

Default Storage location is `/var/opt/morpheus/morpheus-ui/vms`. Additional Storage Providers can be configured in Infrastructure > Storage. Ensure local folders are owned by morpheus-app.morpheus-app if used.

WARNING

Provisioning will fail if Cloud init Enabled is checked and Cloud-Init is not installed on the Image.

NOTE

Existing Image credentials are required for Linux Images that are not Cloud-Init enabled and for Windows Images when Guest Customizations are not used. Cloud-Init and Windows user settings need to be configured in Administration > Settings > Provisioning when using Cloud-Init or Guest Customizations and new credentials are not set on the Virtual Image.

4.

Upload Image

Images can be uploaded by File or URL:

File

Drag and Drop the image file, or select Add File to select the image file.

Url

Select the URL radio button, and enter URL of the Image.

NOTE

The Virtual Image configuration can be saved when using a URL and the upload will finish in the background. When selecting/drag and dropping a file, the image files must upload completely before saving the Virtual Image record or the Image will not be valid.

5. Save Changes.

Subtopics

VMware - VM Templates Copies

VMware - VM Templates Copies

In a VMware environment, you may have a single VM template that you use across different vCenters. Uploading an image to VM Essentials, mentioned in the Add Virtual Image section, is one method to solve this. Alternatively, an organization may decide to create a VM template in one vCenter and then transfer it to other vCenters, which then could be synced into VM Essentials.

If all the vCenters are added as Clouds into VM Essentials and the templates are named the same in each vCenter, they will be aggregated under a single virtual image in VM Essentials. This means that as you deploy to the various vCenter Clouds in VM Essentials using this virtual image, it will choose the correct VM template to use based on the Cloud deployed to.

VM Essentials supports VMware Content Libraries storing VM templates and syncing into VM Essentials, the same as a template in a folder. Additionally, the Content Library can be used to house the same template in multiple libraries. If they have the same name, these templates will be aggregated under a single virtual image. If the Content Library is stored on a datastore that the target host/cluster has access to, it will use that library first, to reduce the cloning time. If the Content Library is not stored in a datastore accessible by the cluster/host, a copy of the VM template will be performed to the target host/cluster instead.

NOTE

VM templates are a **Datacenter** level object. The same process above applies to a single VMware cloud with multiple logical datacenters. It will not apply to clusters, as a template is not associated with a cluster, only when it is converted to a VM.

Infrastructure

The heart of VM Essentials is the ability to manage provisioning across any infrastructure, from bare metal to virtualized clouds and all the way to public infrastructure.

Subtopics

Groups
Clouds
Clusters
Network

Storage
Trust

Groups

Subtopics

Overview
UI
CLI
API
Adding Groups
Managing Groups
Edit Group
Delete Group
User Access

Overview

About this task

Groups in VM Essentials define the available resources for each user. Group access is defined by Roles. Clouds are added to Groups, and a User can only access the Clouds associated with Groups in their Role. Resources such as networks, datastores, resource pools, and folders have additional Group access settings.

The Groups list page displays all current groups, which can be filtered by applied Labels or by simple search. Existing Groups can be edited here and new Groups can be created.

To View Groups:

Procedure

1. Hover over the Infrastructure link in the menu bar
2. Click the Groups link

UI

1. Select the Infrastructure link in the navigation bar
2. Click the Groups link

CLI

To view all groups: `groups list`. To use the group: `groups use <id>` or `groups use "group name"` To get a JSON output of a specific group: `groups get <id> -j` or `groups get "group name" -j`

API

API

To view all groups: `curl https://api.gomorpheus.com/api/groups -H "Authorization: BEARER access_token"` To view a specific group: `curl https://api.gomorpheus.com/api/groups/:id -H "Authorization: BEARER access_token"`

Adding Groups

About this task

To add a group:

Procedure

1. Select the Infrastructure link in the navigation bar
2. Click the Groups link
3. Click the Create Group button
4. Input out the Name and Location (optional) fields
5. Click the Save Changes button to save

Managing Groups

About this task

To view a Group:

Procedure

1. Select the Infrastructure link in the navigation bar
2. Click the Groups link
3. Click the Group name to view/modify

Results

Available tabs in group view

Hosts

: Lists available hosts in the group and displays power, os, name, type, cloud, ip address, nodes, disc space, memory, and status. You can add a host from this tab panel by clicking Add Host.

Virtual Machines

: List all Virtual Machines in the Group.

Bare Metal

: List all Bare Metal Hosts added to the Group

Clouds

: Lists Clouds added to the Group. Existing Clouds or new Clouds can be added from the Group by clicking Add Cloud.

Wiki

: Provides a text area for entering wiki content related to the Group in Markdown format. Additional information on Wiki is available in the Operations_>_Wiki documentation section

Edit Group

About this task

To edit a Group:

Procedure

1. Select the Infrastructure link in the navigation bar.
2. Click the Groups link.
3. Click the name of the group you wish to edit.
4. Click the Edit button.
5. From the Edit Group Wizard modify information as needed.
6. Click the Save Changes button to save.

Delete Group

About this task

To delete a Group:

Procedure

1. Select the Infrastructure link in the navigation bar.
2. Click the Groups link.
3. Click the name of the group you wish to delete.
4. Click the Delete button.
5. Confirm

User Access

IMPORTANT

User access to Groups is determined by their Role(s). Group access for Roles can be configured in the Group Access section of a Role's Settings.

Clouds

Subtopics

Overview

Creating Clouds
Cloud Detail View
Deleting Clouds

Overview

In VM Essentials, a Cloud represents a grouping of HVM clusters (referred to as a “Private Cloud”) or an integration with a VMware vCenter appliance. This section describes general information about the Clouds construct and UI pages for Clouds. See the VMware integration guide for more specific details on integrating with VMware and the features supported by VM Essentials.

Creating Clouds

Clouds can be added from Infrastructure > Clouds or in Infrastructure > Groups > (selected Group) > Clouds. A more detailed guide to adding a VMware vCenter Cloud can be found in the vCenter integration guide. The other available Cloud type, known as Private Cloud, is a generic Cloud type that doesn’t directly integrate with any other technology as the vCenter Cloud type does. Instead Private Cloud-type Clouds are used to house your HVM clusters. Make as many Private Cloud-type Clouds as needed to organize your HVM clusters properly.

Cloud Detail View

The Cloud Detail view shows metrics on health, sync status, resource utilization statistics, and resource counts for hosts, virtual machines, or any other constructs under the umbrella of the selected Cloud.

From the Cloud list page, select the name of a Cloud to display that Cloud’s detail page. You’ll notice the following actions are available:

EDIT

Edit the setup configuration of the Cloud.

REFRESH

Force a sync with the Cloud.

DELETE

Delete the Cloud from VM Essentials.

IMPORTANT

All Instances, managed Hosts, and VMs associated with the Cloud must be removed prior to deleting a Cloud.

Subtopics

Cloud Detail Tabs

Cloud Detail Tabs

NOTE

Not all tabs are available for all Cloud Types.

Clusters

The Clusters tab displays clusters provisioned into the Cloud being viewed, including their status, type, name, layout, workers, and compute, memory, and storage stats. You can add a cluster by clicking ADD CLUSTER.

Hosts

The Hosts tab displays available hosts in the Cloud and displays power, OS, name, type, cloud, IP address, nodes, disk space, memory, and status. You can add a resource by clicking ADD RESOURCE, add a hypervisor host by clicking ADD HYPERVISOR, or perform action an action by selecting one or more Hosts and clicking ACTIONS.

VMs

Displays an inventory of existing Instances in your Cloud configuration and provides details such as power, OS, name, type, cloud, IP address, nodes, disk space, memory, and status.

Bare Metal

Setup PXE Boot in the Boot section to add bare metal servers. Once set up you can view information such as power, OS, name, type, cloud, IP address, nodes, disk space, memory, and status.

Security Groups

The Security Groups tab displays a list of existing security groups in the cloud. You can add a security group to this cloud by clicking EDIT SECURITY GROUPS.

Networks

Displays Networks synced or added to the Cloud, including their name, type, CIDR, pool, DHCP status, visibility and targeted Tenant.

Data Stores

Displays Datastores synced or added to the Cloud, including their name, type, capacity, online status, visibility, and targeted Tenant.

Resources

Displays Resource Pools synced from the Cloud, including their name, description, and targeted Tenant.

Deleting Clouds

About this task

To delete a Cloud:

Procedure

1. Select the Infrastructure link in the navigation bar.
2. Select the Clouds link in the sub navigation bar.
3. Click the Delete icon of the cloud to delete.

Results

IMPORTANT

All Instances, managed Hosts and VMs must be removed prior to deleting a Cloud.

Clusters

Subtopics

Overview
Requirements

Cluster Permissions
HVM clusters

Overview

The Infrastructure > Clusters section is where the list of existing HVM clusters can be viewed. Here you can view high-level statistics about all clusters under management by VM Essentials manager, such as aggregate resource usage by all clusters and the number of workloads running across all of them. Click into an existing HVM cluster to view additional metrics such as hosts, VMs, resource utilization by the host, and a lot more.

Requirements

- VM Essentials Role permission Infrastructure: Clusters > Full required for Viewing, Creating, Editing and Deleting Clusters
- VM Essentials Role permission Infrastructure: Clusters > Read required for Viewing Cluster list and detail pages

Cluster Permissions

- Cluster Permissions

  Each Cluster has Group and Service Plan access permissions settings (Gear icon > Permissionsfrom the Clusters list page)

HVM clusters

An HVM cluster is a hypervisor clustering technology utilizing KVM. Beginning with just a few basic Ubuntu boxes, VM Essentials can create a cluster of HVM hypervisor hosts complete with monitoring, failover, easy migration of workloads across the cluster, and zero-downtime maintenance access to hypervisor host nodes. All of this is backed by a highly-granular RBAC engine, and image library with automation stacks.

Subtopics

Features
Base Cluster Details
Provisioning the Cluster
HVM Cluster Networking
Provisioning a Workload
Monitoring the Cluster
Image Prep (Windows)
Utilizing Existing QCOW Images from an NFS File Share
Hardware Passthrough

Features

Subtopics

Host Features
VM Features

Host Features

- Automated HVM cluster provisioning
- DRS, automatic rebalancing of clusters based on resource consumption
- Compatibility validation of network and storage devices at time of cluster provisioning
- Hypervisor console
- Configuration and deployment of OVS networks (VLANs)
- Cluster and individual host monitoring
- Add hosts to existing clusters
- Console support for cluster hosts
- Add, edit and remove networks and datastores from clusters
- Gracefully take hosts out of service with maintenance mode
- Migration of workloads across hosts
- Configurable automatic failover of running workloads when a host is lost
- Ability to add and provision to fibre channel storage resources or iSCSI storage resources via GFS2 filesystem
- Governance through VM Essentials RBAC
- Pass host-attached NVME, USB, and GPU hardware through to VMs running on the host

VM Features

- Workload provisioning and monitoring (Linux or Windows workloads)
- Console support for running workloads
- Affinity placement, pin VMs to hosts
- Brownfield discovery of existing VMs
- Reconfigure VM sizing
- Disk migration across datastores
- UEFI support
- Migration of VMs across hosts
- Configure automatic failover for individual VMs in the event a host is lost
- Reconfigure running workloads to resize plan, add/remove disks, and add/remove network interfaces
- Backup and restore VM workloads, with optional synthetic full backups
- Clone VMs
- Take snapshots and revert to snapshots

- VM Essentials library and automation support
- Claim and consume host-attached NVME, USB, and GPU hardware to run hardware-accelerated workloads on VMs

Base Cluster Details

An HVM cluster using the hyperconverged infrastructure (HCI) Layout consists of at least three hosts. Physical hosts are recommended to experience full performance of the solution. In smaller environments, it is possible to create an HVM cluster with three nested virtual machines, a single physical host (non-HCI only), or a single nested virtual machine (non-HCI only) though performance may be reduced. With just one host it won't be possible to migrate workloads between hosts or take advantage of automatic failover. Currently, the default cluster layout requires hosts be a pre-existing Ubuntu 24.04 box with environment and host system requirements described in this section. An earlier cluster layout requiring Ubuntu 22.04 is also included. VM Essentials handles cluster configuration by providing the IP address(es) for your host(s) and a few other details. Details on adding the cluster to VM Essentials are contained in the next section.

Subtopics

Hardware Requirements
Example Cluster Deployment

Hardware Requirements

- **Operating System:** Ubuntu 24.04 or Ubuntu 22.04
- **CPU:** One or more 64-bit x86 CPUs, 1.5 GHz minimum with Intel VT or AMD-V enabled
- **Memory:** 4 GB minimum. For non-converged Layouts, configure HVM hosts to use shared external storage, such as an NFS share or iSCSI target.
- **Disk Space:** For converged storage, a data disk of at least 500 GB is required for testing. More storage will be needed for production clusters. An operating system disk of 15 GB is also required. Clusters utilizing non-converged Layouts can configure external storage (NFS, etc.).
- **Network Connectivity:** HVM hosts must be assigned static IP addresses. They also need DNS resolution of the VM Essentials appliance and Internet access in order to download and install system packages for dependencies, such as KVM, Open vSwitch (OVS), and more

NOTE

Ubuntu 22.04 uses `netplan` for networking and it is the responsibility of the customer to establish recommended networking configurations prior to provisioning an HVM cluster. To configure a static IP address, change into the directory holding the config files (`cd /etc/netplan`) and edit the existing configuration file (`/etc/netplan/50-cloud-init.yaml` or `/etc/netplan/00-installer-config.yaml` or `/etc/netplan/01-netcfg.yaml`). If desired, backup the existing configuration prior to editing it (`cp /etc/netplan/<file-name>.yaml /etc/netplan/<file-name>.yaml.bak`). For additional information on configuration file formatting, refer to `netplan` **documentation**. Once the configuration is updated, validate and apply it (`netplan try`). The `try` command will validate the configuration and apply it if it's valid. If invalid, it will automatically be rolled back.

NOTE

Clustered storage needs as much network bandwidth as possible. Network interfaces of at least 10 Gbps with jumbo frames enabled are required for clustered storage and for situations when all traffic is running through the management interface (when no compute or storage interface is configured). It's highly likely that performance will be unacceptable with any lower configurations.

Table 1. Network Communication Ports

Description	Source	Destination	Port	Protocol
VM Essentials Agent communication with the VM Essentials appliance	HVM host	VM Essentials appliance server	443	TCP
HVM host configuration and management	VM Essentials appliance server	HVM host	22	TCP
Inter-host communication for clustered deployments	HVM host	HVM host	22	TCP
VM Essentials server SSH access for deployed virtual machines	VM Essentials appliance server	Hosted virtual machines	22	TCP
VM Essentials server WinRM (HTTP) access for deployed virtual machines	VM Essentials appliance server	Hosted virtual machines	5985	TCP
VM Essentials server WinRM (HTTPS) access for deployed virtual machines	VM Essentials appliance server	Hosted virtual machines	5986	TCP

Example Cluster Deployment

In this example cluster, each host box consists of:

- 4 vCPU
- 16 GB memory
- 20 GB OS boot disk
- 250 GB data disk (deployed to `/dev/sdb`)
- 3 network interfaces for management, storage, and compute traffic (set to `eth0`, `eth1`, and `eth2`, respectively, in this example. Your environment may differ.)

NOTE

250 GB data disks used in this example are simply for demonstration purposes. A typical test cluster should consist of at least 500 GB storage and more will be required for production. Do not raid disks on physical servers. Multiple disks may be specified per host by giving a comma-separated list (ex. /dev/sda,/dev/sdb,/dev/sdc,etc.) in the DATA DEVICE field during cluster setup. These along with disks from all other nodes will be added to the total storage, which is presented as one large volume.

HVM clusters must also live in Private Cloud-type Clouds (See Infrastructure > Clouds). A pre-existing Cloud may be used or a new Cloud could be created to house HVM clusters.

Provisioning the Cluster

As mentioned in the previous section, HVM hosts should be running Ubuntu 24.04 to use the latest HVM cluster layout (version 1.2+). HVM hosts running Ubuntu 22.04 can also be used (select HVM cluster layout 1.1). I also have a Private Cloud-type Cloud to house the cluster. Begin the cluster creation process from the Clusters list page (Infrastructure > Clusters). Click + ADD CLUSTER and select "HVM".

VM Essentials gives the option to select a hyperconverged infrastructure (HCI) **LAYOUT** or non-HCI. In this example, the HCI Layout is used (requires a three-node minimum). Next, configure the names and IP addresses for the host boxes (**SSH HOST**). The SSH HOST name configuration is simply a display name in VM Essentials, it does not need to be a hostname. By default, configuration space is given for three hosts which is what this example cluster will have. You must at least configure one and it's possible to add more by clicking the (+) button. The **SSH PORT** is pre-configured for port 22, change this value if applicable in your environment. Next, set a pre-existing user on the host boxes (**SSH USERNAME** and **SSH PASSWORD**) and **SSH KEY**. Use a regular user with sudo access.

In the next part of the modal, you'll configure the storage devices and network interfaces. Find your disk name, if needed, with the `lsblk` command. In my case, the target device is located at `/dev/sdb`.

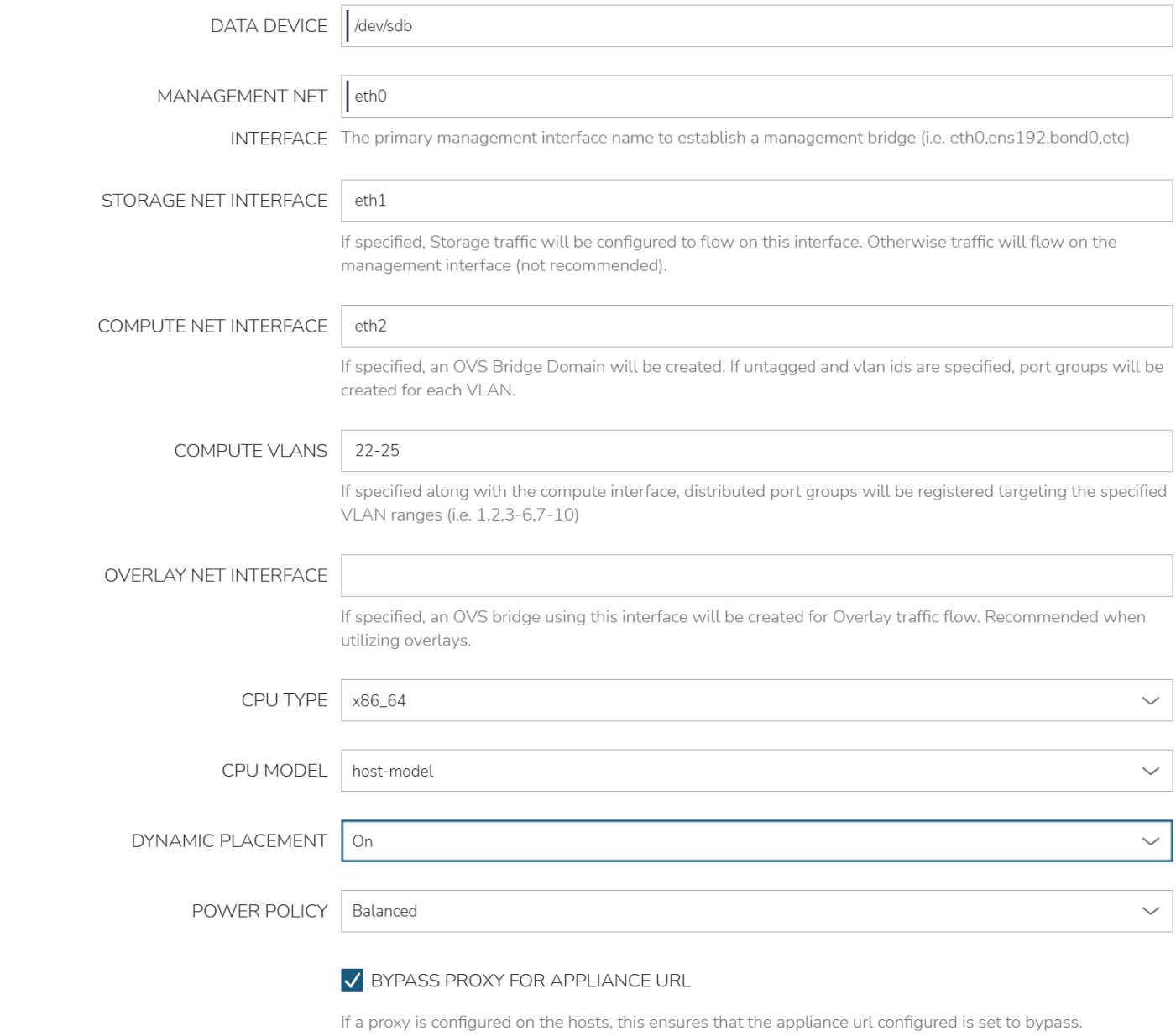
Though not strictly required, it's recommended to have separate network interfaces to handle cluster management, storage traffic, and compute. In this example case, `eth0` is configured as the **MANAGEMENT NET INTERFACE** which handles communication between the cluster hosts. `eth1` is configured as the **STORAGE NET INTERFACE** and `eth2` is configured as the **COMPUTE NET INTERFACE**. The **COMPUTE VLANS** field can take a single value (ex. 1) or a range of values (ex. 22-25). This will create OVS port group(s) selectable as networks when provisioning workloads to the cluster. If needed, you can find your network interface names with the `ip a` command.

Next, only one **CPU TYPE** is currently supported (`x86_64`) though this may change in the future. For **CPU MODEL** configuration, we surface the entire database of model configurations from `libvirt`. If unsure or if you don't know of a specific reason to choose one or the other, select `host-passthrough` which is the default option.

Finally, select a **DYNAMIC PLACEMENT** and **POWER POLICY**configuration. When enabled, Dynamic Placement will automatically balance VMs across cluster hosts based on resource utilization. When disabled, VMs will only migrate to a new host if they are pinned to a specific host or failed over and not running on the preferred host. With Power Policy, set Balanced (default) or Performance configuration. Balanced optimizes for a mix of performance and efficiency. Performance mode is optimized for scenarios requiring maximum performance. It reduces network latency by applying configurations similar to the `tuned` "network-latency" profile and switches CPUs into performance mode.

NOTE

Power Policy settings require Agent version 3.0.0+ running on the HVM Host and take effect following the next sync cycle. You can upgrade HVM Host Agents by navigating to the Host detail page, opening the ACTIONS menu, and selecting Upgrade Agent. Alternatively, you can select Download Agent Script to download a script which can be run on the HVM Host to upgrade its Agent version. Download scripts are specific to the HVM Host so you will need an individual script per HVM Host. Power Policy settings will persist following a HVM Host reboot.


DATA DEVICE
/dev/sdb
MANAGEMENT NET
eth0
INTERFACE
The primary management interface name to establish a management bridge (i.e. eth0,ens192,bond0,etc)
STORAGE NET INTERFACE
eth1
If specified, Storage traffic will be configured to flow on this interface. Otherwise traffic will flow on the management interface (not recommended).
COMPUTE NET INTERFACE
eth2
If specified, an OVS Bridge Domain will be created. If untagged and vlan ids are specified, port groups will be created for each VLAN.
COMPUTE VLANS
22-25
If specified along with the compute interface, distributed port groups will be registered targeting the specified VLAN ranges (i.e. 1,2,3-6,7-10)
OVERLAY NET INTERFACE
If specified, an OVS bridge using this interface will be created for Overlay traffic flow. Recommended when utilizing overlays.
CPU TYPE
x86_64
CPU MODEL
host-model
DYNAMIC PLACEMENT
On
POWER POLICY
Balanced
BYPASS PROXY FOR APPLIANCE URL
If a proxy is configured on the hosts, this ensures that the appliance url configured is set to bypass.

At this point we've kicked off the process for configuring the cluster nodes. Drill into the Cluster detail page and click on the History tab. Here we can monitor the progress of configuring the cluster. HPE Morpheus VM Essentials will run scripts to install KVM, install OVS, and to prepare the cluster. In just a short time, the cluster provisioning should complete and the cluster will be ready to deploy workloads.

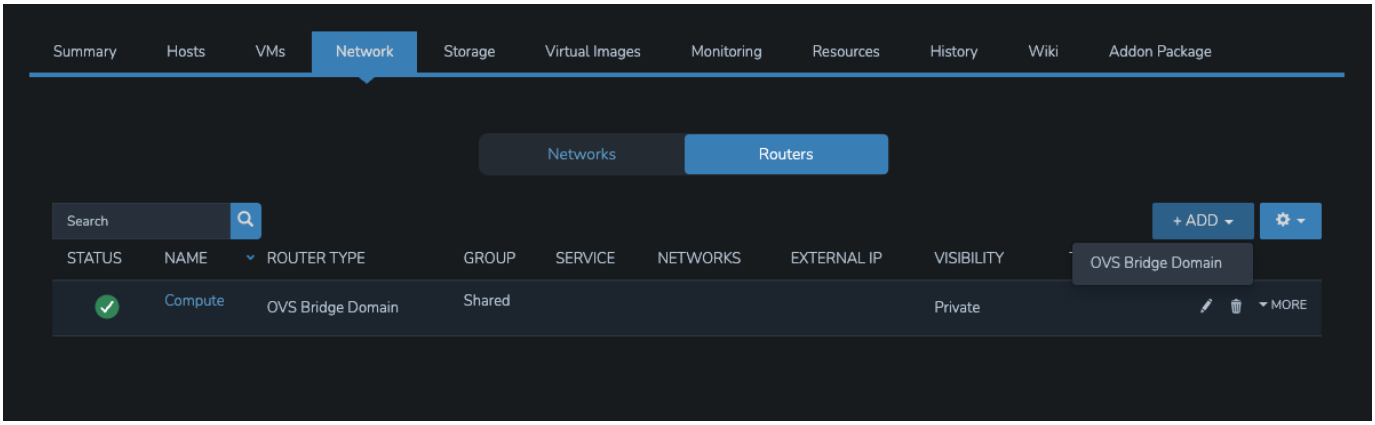
HVM Cluster Networking

On initial cluster provisioning, OVS bridges and Libvirt Networks are created and are immediately ready for VM provisioning. However, when adding new network interfaces, you may need to create networking objects in the UI manually. Currently, the HPE Morpheus VM Essentials Software Manager does not discover new interfaces that are not in netplan. You'll need to ensure they are in the `01-base.yml` netplan file, apply it, create the bonds in the `hpe-vm` tool, and then refresh the HVM Cluster via the UI. See the installation section at the beginning of this documentation repository for more information on the `hpe-vm` tool and its use.

HVM network objects are created from the Network tab of the HVM Cluster detail page (Infrastructure > Clusters, then select the HVM Cluster). Two subtabs are shown here for Routers and Networks. From a KVM perspective, OVS Bridges and Libvirt Networks (without any port groups) are created on the Routers subtab. Port Group entries are added to existing Libvirt Networks on the Networks subtab. For this reason, it's often most logical to begin creating new HVM network objects on the Routers subtab before moving onto the Networks subtab. For a higher level discussion and diagram of recommended HVM Cluster network topology and to see where these objects fit in, refer back to the example network configurations in the "Getting Started" section of this user manual.

Adding Routers

1. From the Routers subtab, click + ADD, then select OVS Bridge Domain



2. On the ADD NETWORK ROUTER modal, configure the following:

   a. **GROUP:** Select "Shared" to make the router object available to all Groups or select an individual Group

   b. **NAME:** A name for the router object in HPE Morpheus VM Essentials Software

   c. **HOST BRIDGE:** Select an existing OVS bridge or choose "Create New"

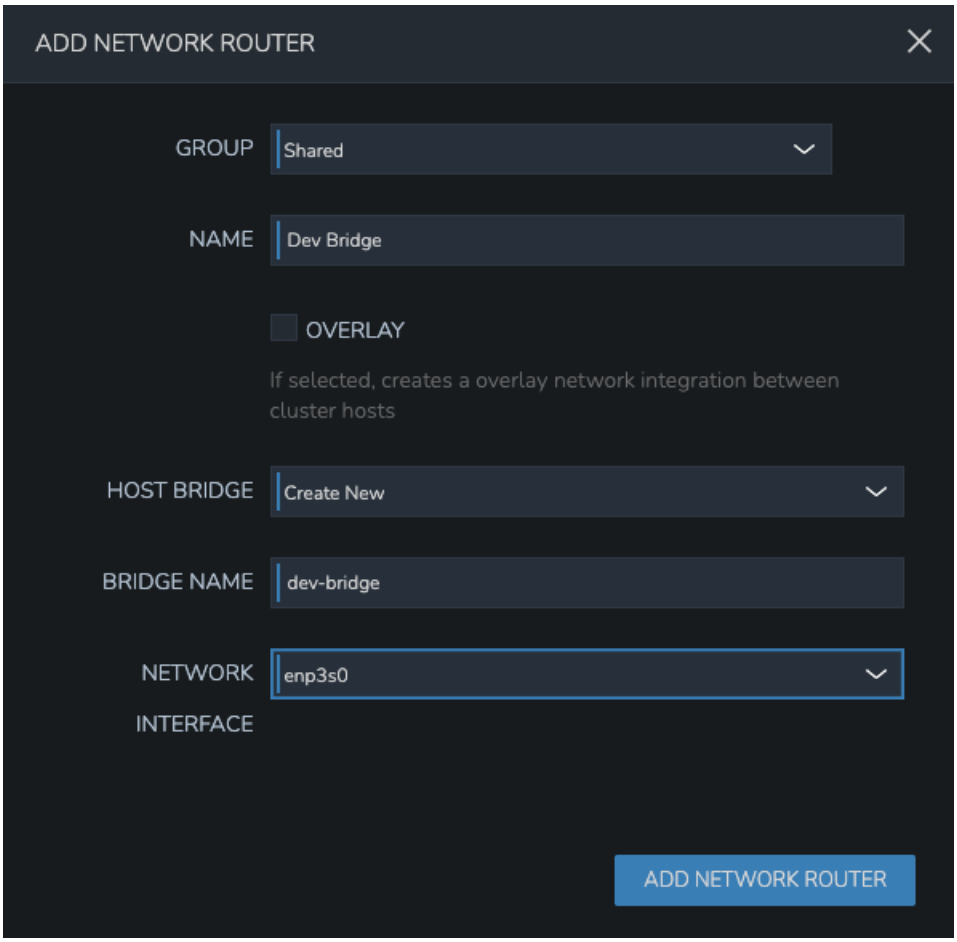
   d. **BRIDGE NAME:** Shown only when opting to create a new Host Bridge. Provide a name for the new OVS bridge to be created. The bridge name value entered here will be used to identify the bridge throughout the UI while examining the created objects via a terminal session connected to the Host will show it identified by the interface name

   e. **NETWORK INTERFACE:** Shown only when opting to create a new Host Bridge. Select a network interface for the new OVS bridge. Keep in mind that currently new interfaces are not discovered automatically. See the opening paragraph of this section for more information on surfacing the new interface to the HVM Cluster

   NOTE

   By adding a router here and selecting an existing OVS bridge, a new Libvirt Network is created without any port groups but no new OVS bridge is created. When selecting "Create New" in the Host Bridge configuration field, a new OVS bridge is created and a new Libvirt Network is also created without any port groups. A free physical interface or bond must be available to create a new OVS bridge and currently these are not automatically discovered by the HVM Cluster. See the opening paragraph of this section for more information on surfacing new interfaces to the HVM Cluster. Libvirt Port Groups are created in the next section on adding networks. For a higher level discussion and diagram of recommended HVM Cluster network topology and to see where these objects fit in, refer back to the example network configurations in the "Getting Started" section of this user manual.

3. Click ADD NETWORK ROUTER

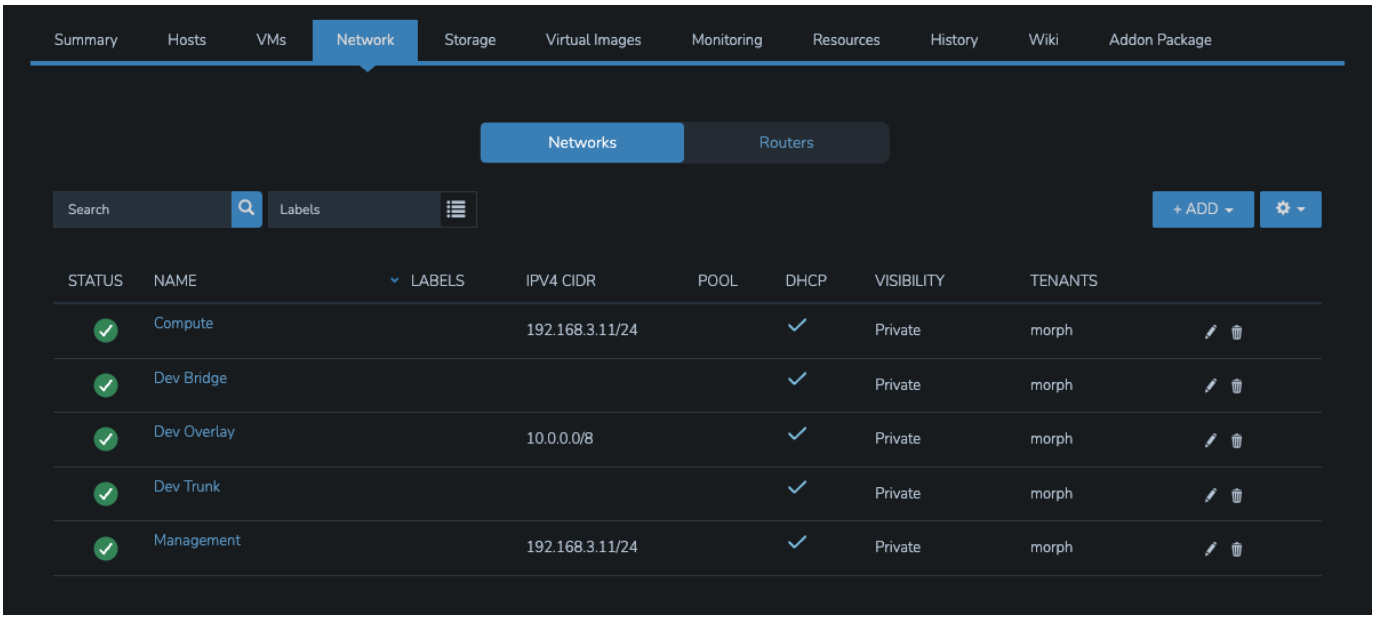


Once saved, the router object is created and it appears in the list of current routers.

Adding Networks

As mentioned in the previous section, creating network objects on HVM clusters is akin to adding Libvirt Portgroups to an existing Libvirt Network. If continuing from the previous section on adding routers, the OVS bridges and Libvirt networks will be in place to add port groups (referred to as networks here in the UI).

1. From the Networks subtab, click + ADD, then select OVS Port Group



2. On the CREATE NETWORK modal, configure the following:

a. **GROUP:** Select "Shared" to make the router object available to all Groups or select an individual Group

b. **NAME:** A name for the network object in HPE Morpheus VM Essentials Software

c. **CIDR:** The CIDR range for the new network

d. **GATEWAY:** The network gateway address

e. **DNS PRIMARY:** The address for the primary DNS server

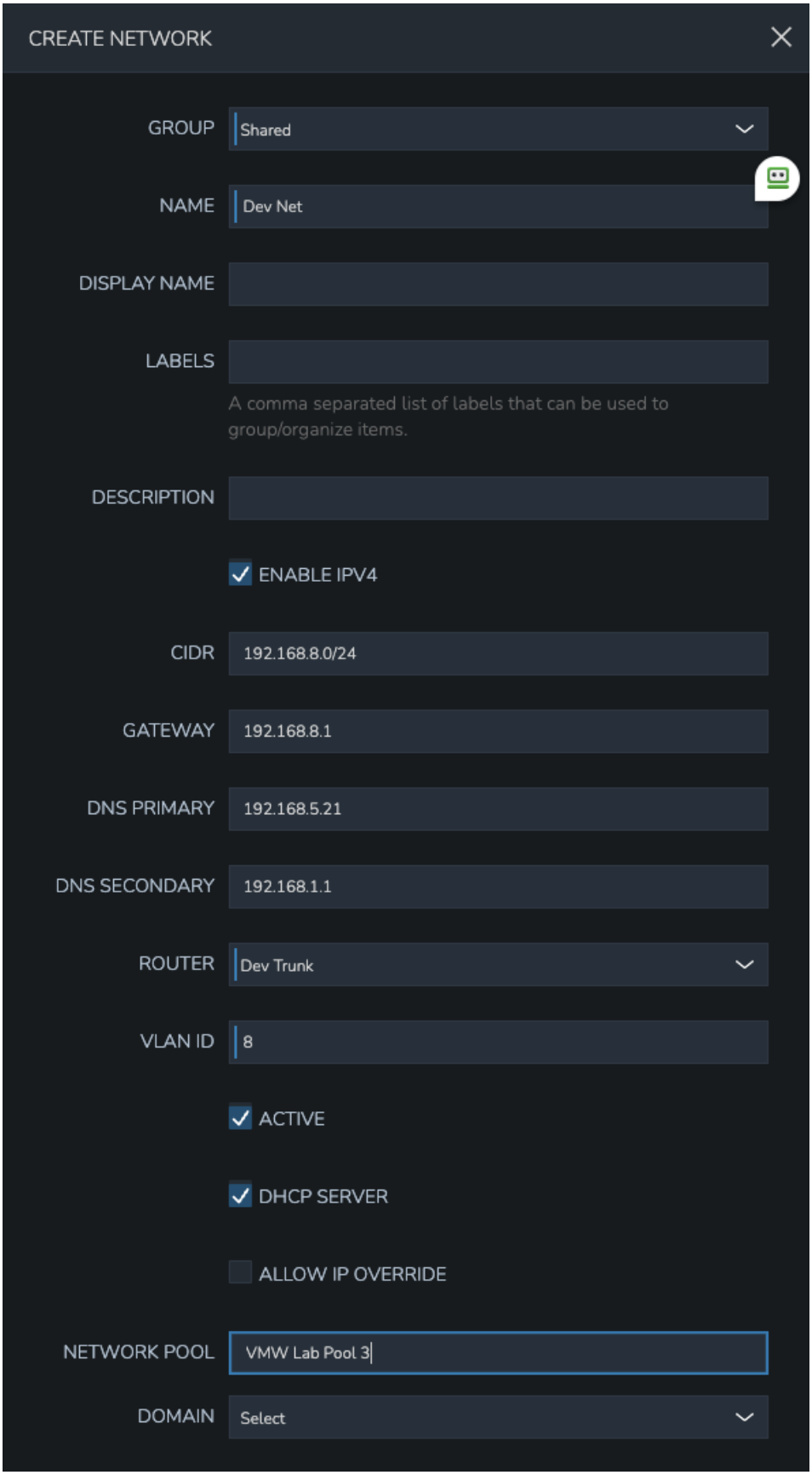
f. **DNS SECONDARY:** The address for the secondary DNS server

g. **ROUTER:** Select an existing OVS bridge. If you need to create a new OVS bridge, add a new "OVS Bridge Domain" from the Routers subtab (described above) and select "Create New" for it's "Host Bridge" field configuration. Additional details on router objects are provided above.

h. **VLAN ID:** A VLAN ID for the Libvirt Port Group to be created

i. **NETWORK POOL:** A typeahead field for selecting a currently-configured IP Pool

3. Click SAVE CHANGES



Provisioning a Workload

At this point, the cluster is ready for workloads to be provisioned to it. Within the Instance provisioning wizard (See Provisioning > Instances

documentation for more details on provisioning), there is now the “HVM” Instance Type. This Instance will allow you to choose from any HVM cluster-compatible images within your environment. Out of the box, VM Essentials does not include any compatible images but there is a section later in this guide covering the process of onboarding existing QCOW images into the UI as Virtual Images and another section covering the process of prepping Windows images from the downloaded ISO.

After arriving at the Configure tab of the provisioning wizard, select a Plan based on resource needs. From the **RESOURCE POOL** field, select the desired HVM cluster. When configuring **VOLUMES** for the new workload, note that space can be claimed from the configured volume. Within **NETWORKS**, we can add the new workload to one of the **VLANS** set up as part of cluster creation. Finally, note that we can choose the HOST the workload should run on in addition to selecting the compatible image.

TIP

The VOLUMES configuration within the provisioning wizard includes a flyout menu allowing storage type (standard, thin, thick (lazy zero), and thick (eager) and storage profile (cache: none or cache: directsync) configurations to be set on each individual volume.

Review and complete the provisioning wizard. After a short time, the workload should be up and running. With a workload now running on the cluster, we can take a look at some of the monitoring, migration, failover, and other actions we can take for workloads running on HVM clusters.

NOTE

HVM clusters support CPU pinning (tying specific vCPUs associated with running workloads to specific physical CPU cores). Currently, this must be done manually by accessing the appropriate HVM host and issuing `virsh` commands or editing XML. Adding UI tools to view and control CPU pinning is on the product roadmap to be added in the near future. Despite the requirement to edit CPU pinning manually, this is a supported action for workloads running on HVM clusters.

Monitoring the Cluster

With the server provisioned and a workload running, take a look at the monitoring and actions capabilities on the cluster detail page (Infrastructure > Clusters, then click on the new HVM cluster). View cluster performance and resource usage (Summary and Monitoring tabs), drill into individual hosts (Hosts tab), see individual workloads (VMs tab), and more.

Subtopics

- Moving Workloads Between Hosts
- Adding hosts
- Maintenance Mode
- Affinity Groups
- Failover
- Adding an NFS Datastore

Moving Workloads Between Hosts

To manually move workloads between hosts, drill into the detail page for the VM (from the VMs tab of the cluster detail page). Click ACTIONS and select “Manage Placement”. Choose a different host and select from the following placement strategies:

- **Auto:** Manages VM placement based on load
- **Failover:** Moves VMs only when failover is necessary
- **Pinned:** Will not move this workload from the selected host

Within a short time, the workload is moved to the new host.

Adding hosts

The process of adding hosts to a pre-existing cluster is very similar to the process of provisioning the cluster initially. The requirements for the new worker node will be identical to the nodes initially added when the cluster was first provisioned. See the earlier sections in this guide for additional details on configuring the worker nodes.

To add the host, begin from the Cluster detail page (selected from the list at Infrastructure > Clusters). From the Cluster detail page, click ACTIONS and select “Add Worker”. Configurations required are the same as those given when the cluster was first created. Refer to the section above on “Provisioning the Cluster” for a detailed description of each configuration.

Once VM Essentials has completed its configuration scripts and joined the new worker node to the cluster, it will appear in a ready state within the Hosts tab of the Cluster detail page. When provisioning workloads to this Cluster in the future, the new node will be selectable as a target host for new Instances. It will also be an available target for managing placement of existing VMs running on the cluster.

NOTE

It’s useful to confirm all scripts related to creating the new host and joining the new host to the cluster completed successfully. To confirm, navigate to the detail page for the new host (Infrastructure > Clusters > Selected Cluster > HostsTab > SelectedHost) and click on the History tab. Confirm all scripts, even those run on the pre-existing hosts, completed successfully as it’s possible the new host was added successfully (green status) but failed in joining the cluster. When such a situation occurs it may appear adding the new host was successful though it will not be possible to provision workloads onto it due to not joining the cluster successfully.

Maintenance Mode

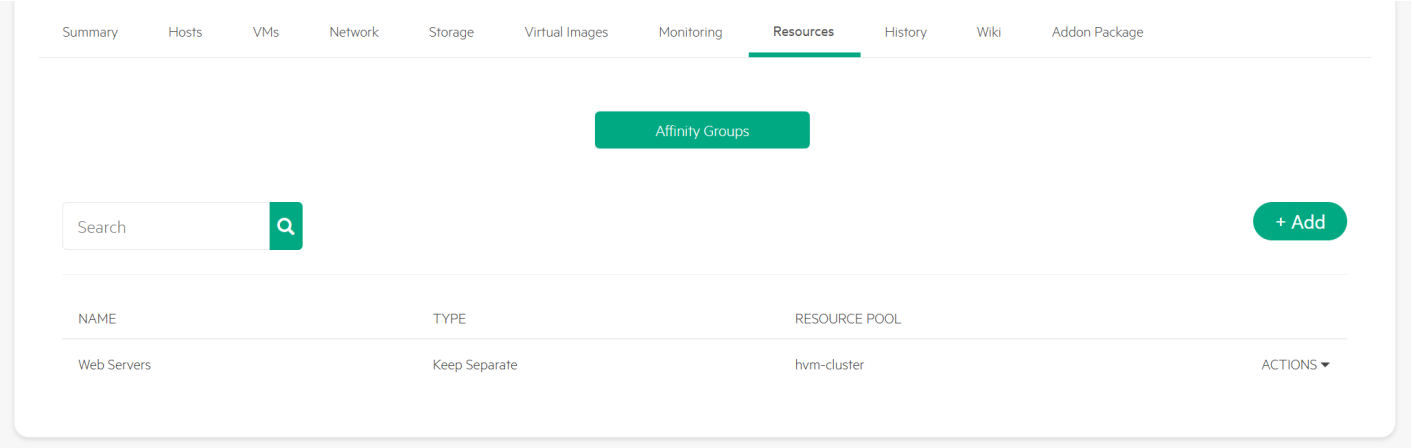
HVM hosts can be easily taken out of service for maintenance when needed. From the host detail page, click ACTIONS and then click “Enter Maintenance.” When entering maintenance mode, the host will be removed from the pool. Live VMs that can be migrated will be moved to new hosts. VMs that are powered off will also be moved when possible. When a live VM cannot be moved (such as if it’s “pinned” to the host), the host will not go into maintenance mode until that situation is cleared. You could manually move a VM to a new host or you could power it down if it’s non-essential. After taking that action, attempt to put the host into maintenance mode once again. VM Essentials UI provides a helpful dialog which shows you which VMs live on the host are to be moved as the host goes into maintenance mode. When maintenance has finished, go back to the ACTIONS menu and select “Leave Maintenance.”

Affinity Groups

HVM Clusters offer affinity groups and anti-affinity groups. These work similarly to affinity groups on other platforms, such as the affinity rules concept in VMware vSphere. An affinity group contains a type (either Keep Together or Keep Separate) and a list of servers which should have the rule applied. Whenever possible, servers configured to "Keep Together" will run on the same HVM Host. Servers configured to "Keep Separate" will be balanced across HVM Hosts to the maximum extent possible.

Viewing Affinity Groups

Affinity groups are listed on the Resources tab of the HVM Cluster detail page (Infrastructure > Clusters, then select the appropriate HVM Cluster). From the ACTIONS menu for each affinity group, they may be edited or deleted. By editing an affinity group, users may view or edit its enabled status (affinity groups which are not enabled will not be acted on).



Adding Affinity Groups

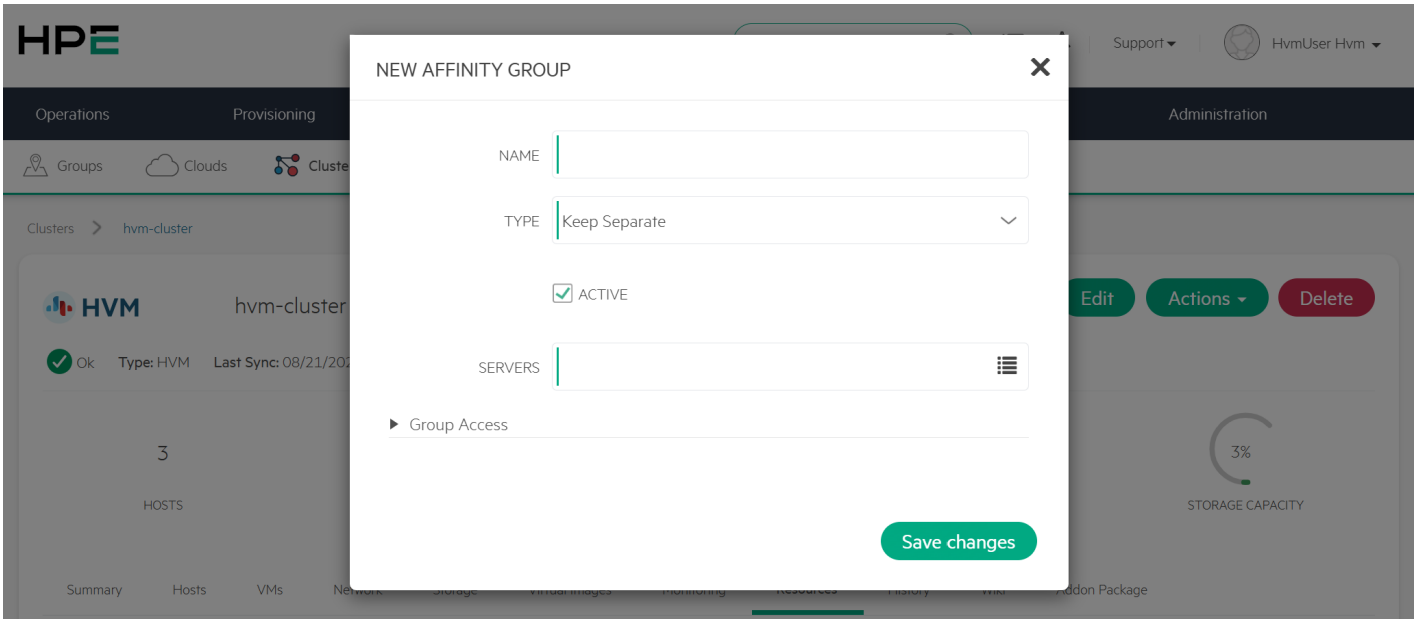
As mentioned in the previous section, affinity groups are listed on the Resources tab of the HVM Cluster detail page (Infrastructure > Clusters, then select the appropriate HVM Cluster). From here, to create a new affinity group, click + ADD. Configure the following:

- **NAME:** A name for the affinity group
- **TYPE:** Select either "Keep Together" or "Keep Separate" to indicate whether the selected servers should run on as few or as many servers as possible within the capabilities of the HVM Cluster
- **ACTIVE:** When checked, the rules defined in the affinity group will be applied to the HVM Cluster
- **SERVERS:** Select as many servers as desired from the typeahead list

Once finished, click SAVE CHANGES. Following the next cluster sync, the affinity rule will be applied and VMs will begin to migrate (if applicable).

TIP

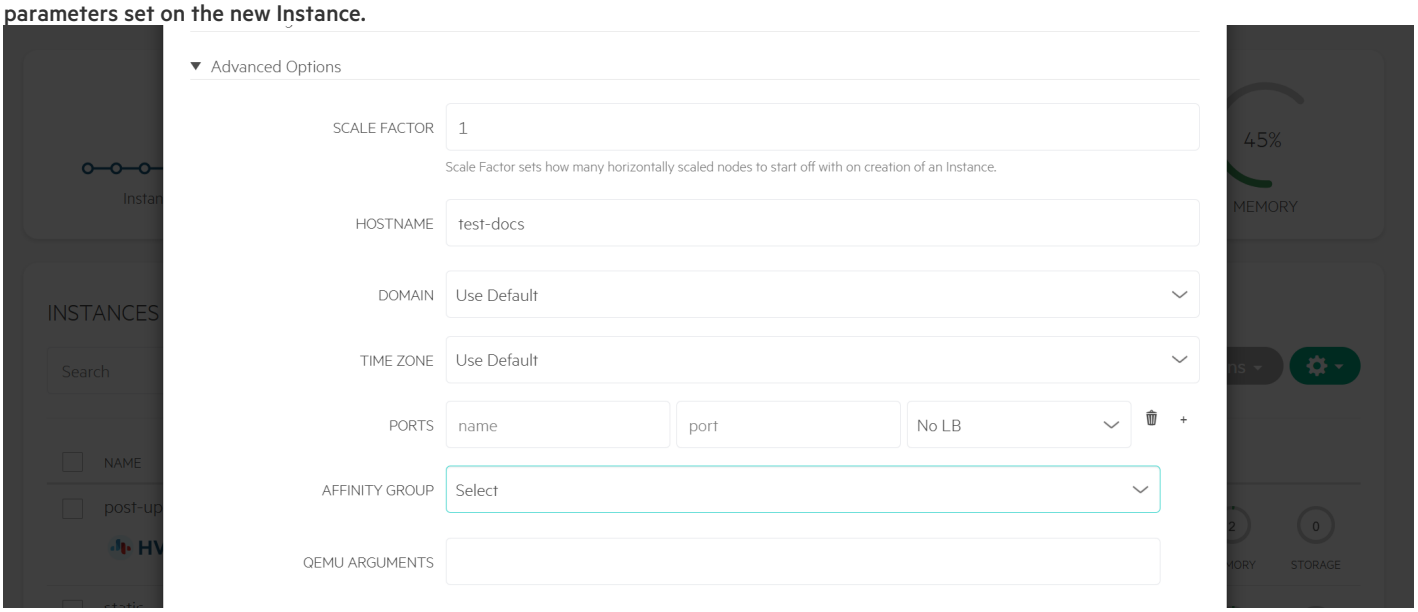
Placement settings (ex. pinning a VM to a specific host) can override an affinity group. HVM Clusters will attempt to implement affinity groups intelligently to work around VM placement. For example, in a group of five VMs configured to "keep together" with one pinned to host 1, the Cluster would run all five VMs on host 1 (if possible) to simultaneously honor the placement and the affinity group. In some scenarios, it will not be possible to simultaneously honor all placements and affinities/anti-affinities.



Adding Servers to Affinity Groups at Provision Time

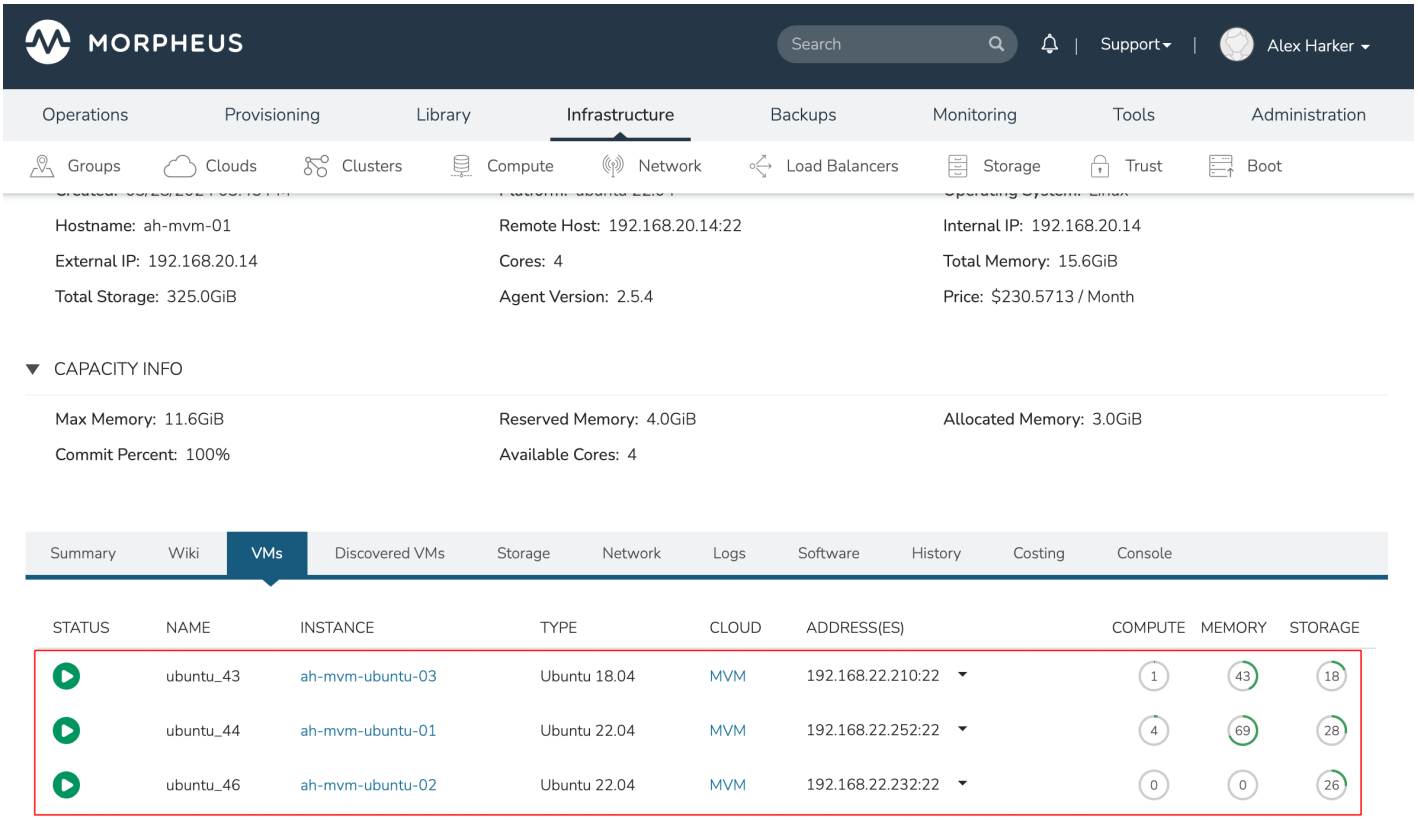
In addition the adding servers from the affinity group, newly-provisioned servers may be added to an affinity group at provision time. From the CONFIGURE tab of the provisioning wizard, expand the Advanced Options section. Within Advanced Options, select an affinity group. The affinity group must be pre-existing and this list will be filtered to show only affinity groups that apply depending on other configuration

parameters set on the new Instance.

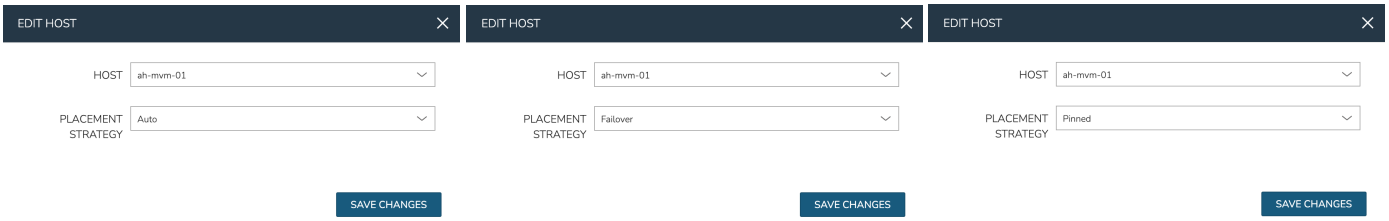


Failover

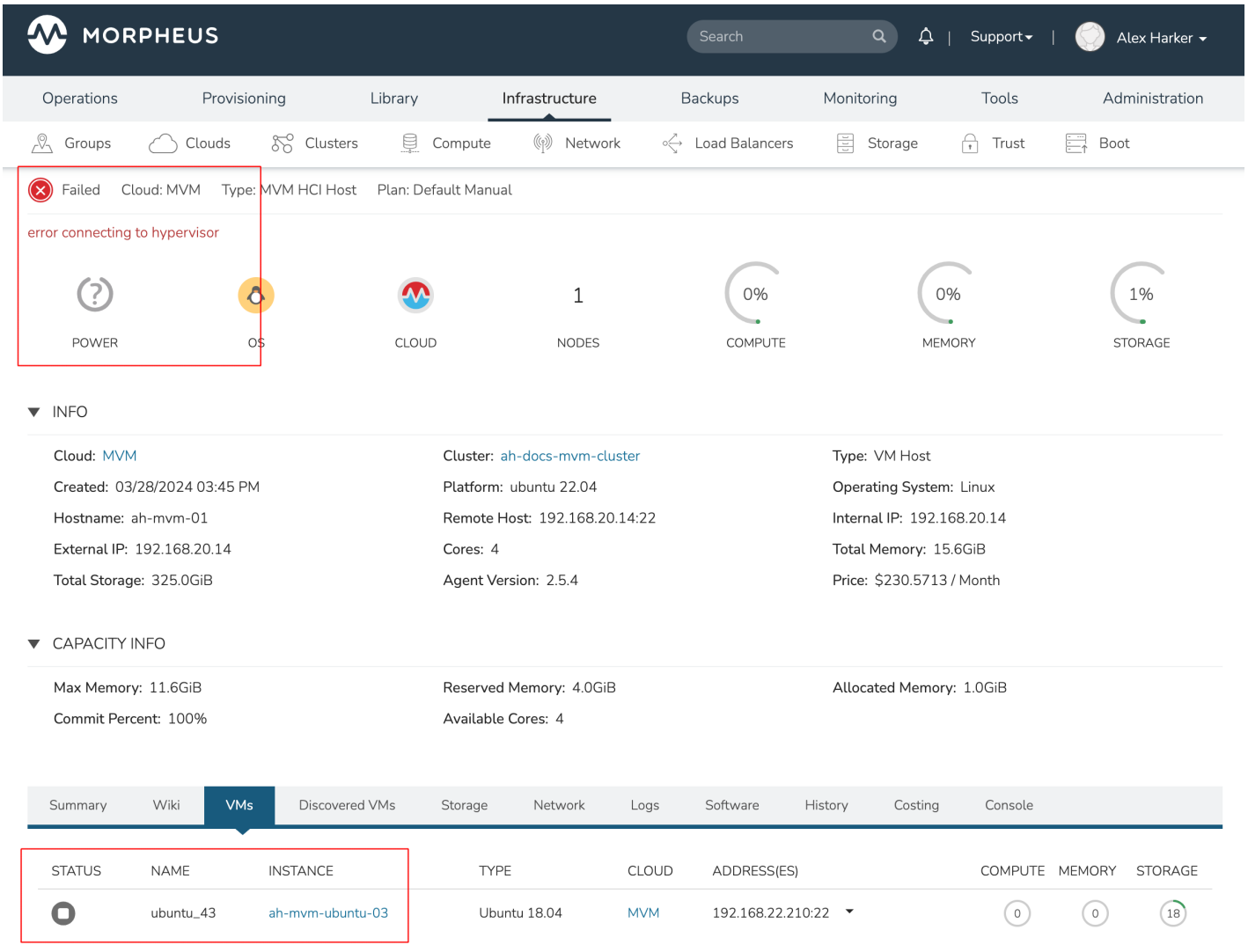
HVM clusters support automatic failover of running workloads in the event of the loss of a host. Administrators can control the failover behavior through the “Manage Placement” action on any running VM. From the VM detail page, click ACTIONS and select “Manage Placement”. Any VM with a placement strategy of “Auto” or “Failover” will be eligible for an automatic move in the event its host is lost. When the loss of a host does occur, the workload will be up and running from a different cluster host within just a short time if it’s configured to be moved during an automatic failover event. Any VMs pinned to a lost host will not be moved and will not be accessible if the host is lost. When the host is restored, those VMs will be in a stopped state and may be restarted if needed.

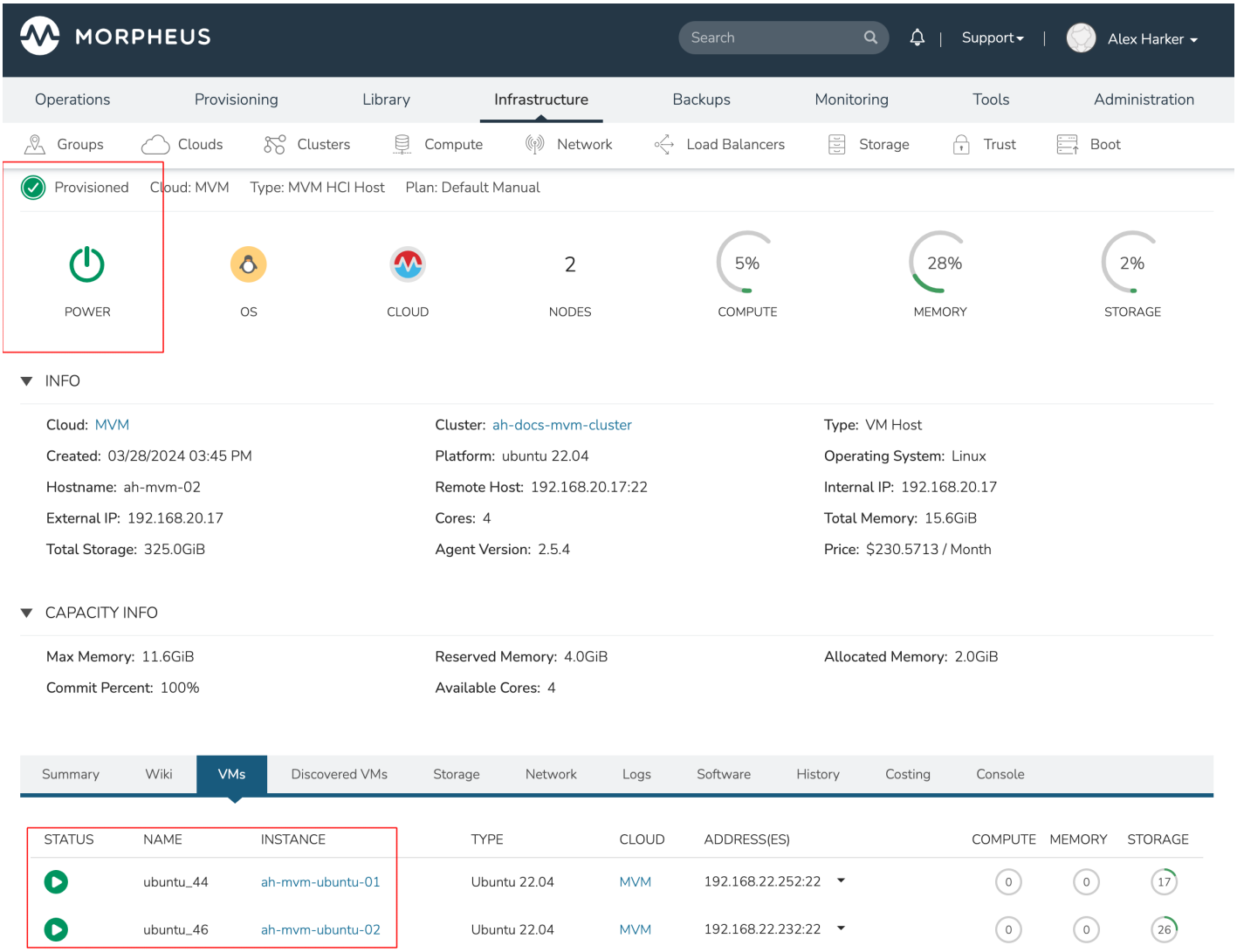


Each of these VMs is configured for a different failover strategy. When the host is lost, we should expect to see the first two VMs moved to an available host (since they have the “Auto” and “Failover” placement strategies, respectively). We should not see the third VM moved.



After loss of the host these three VMs were running on, we can see the lost host still has one associated VM in a stopped state. The other two VMs are running on a second host which is still available.





When the lost host returns, the moved VMs will come back to their original host. The third VM is associated with this host as well and is in a stopped state until it is manually restarted.

Adding an NFS Datastore

Existing NFS shares can be used with HVM clusters for virtual machine storage. These are added and viewed from the Storage tab of the cluster detail page and, once added and active, become selectable as targets for virtual machine storage.

NOTE

Ensure NFS is properly configured to allow all of the HVM hosts to access the shared directory, including permissions to read and write. For backup purposes, it's also helpful to give VM Essentials access to NFS.

Start by navigating to the Storage tab of the cluster detail page. Make sure the Data Stores subtab is also selected. Here you will see a list of existing datastores with some additional information, such as type, capacity, and status. Click ADD. Enter the NAME for the datastore in VM Essentials and select the TYPE as NFS Pool. Note that the datastore name cannot be changed once it has been created. This will update the available fields to include the additional fields needed to integrate the NFS server. Enter the SOURCE HOST which is the hostname or the IP address of the NFS server. Finally, enter the SOURCE DIRECTORY which is the directory path of the NFS share. Click SAVE.

Once the modal is saved, it will take a few minutes to initialize the new datastore and show a successful online status in VM Essentials. Once this initialization process is completed, the datastore can now be used as VM storage for cluster.

Image Prep (Windows)

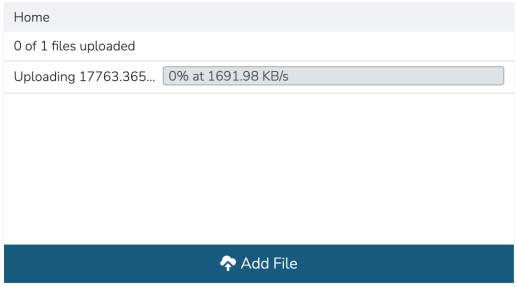
This section will go through the steps to prepare a Windows image which can be successfully provisioned to HVM clusters. Additionally, this image can serve as a template from which additional images and VM Essentials Library items can be built. In this example case, we'll start from downloading a Windows Server 2019 ISO directly from the Microsoft download center and go all the way through to creating a new Instance Type in VM Essentials that users can provision on-demand.

With the Windows ISO already downloaded, begin by uploading the ISO as a Virtual Image in VM Essentials. Virtual Images are added in Library > Virtual Images. Click + ADD and then choose "ISO." Before adding the file itself, set the following configurations on the Virtual Image:

- **NAME:** A name for the Virtual Image in VM Essentials, such as "Windows Server 2019 ISO"
- **OPERATING SYSTEM:** "windows server 2019"
- **MINIMUM MEMORY:** Filters out Service Plans at provision time which do not meet the minimum value. For this image type, I've set 4 GB

In addition to the above, there are a number of checkbox configurations here (many of them are in the expandable "Advanced" section), some of which are checked by default. They should all be unchecked except for "VIRTIO DRIVERS LOADED?" within the "Advanced" expandable section.

With the configurations set, it's time to upload the ISO to VM Essentials. Keep in mind that if you do not specify a bucket in which the file should be uploaded, it will be uploaded to the appliance itself. If you choose to do this, be sure you have enough space to store the images you need. Within the UPLOAD VIRTUAL IMAGE modal is a large dropzone labeled "Drop Files Here." You can drag and drop the ISO file here or you can click the button labeled "Add File" and browse for it. A progress bar will appear, wait until the file is completely uploaded before you save and dismiss the modal. After the file has completely uploaded, click SAVE CHANGES.

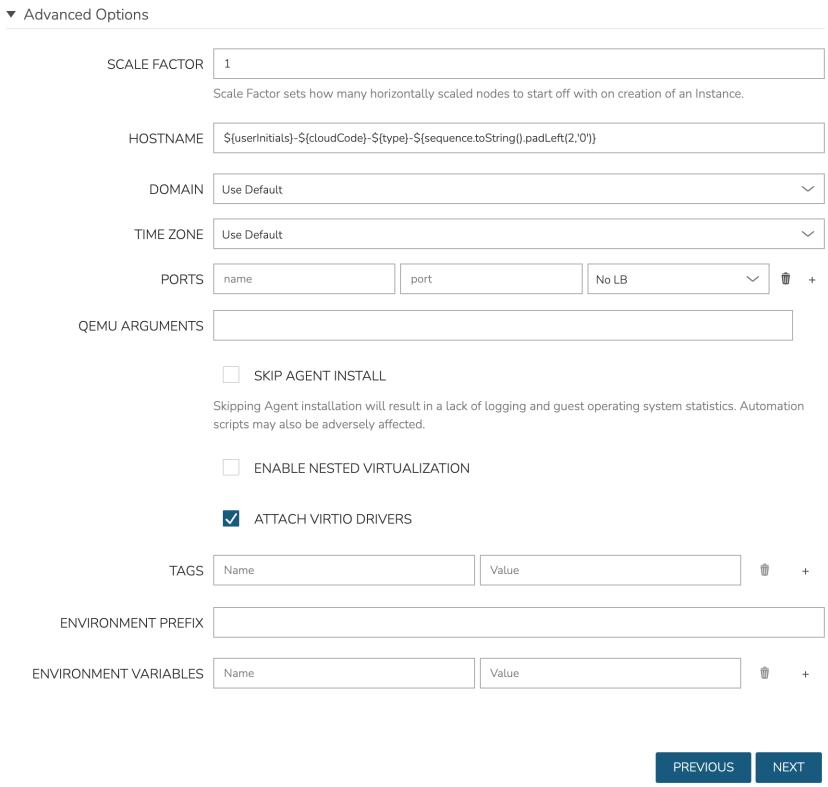


Next, we'll provision a VM from the ISO using the built-in HVM Instance Type. Once running, we will configure the VM to any specific requirements and convert it to a template. Navigate to Provisioning > Instances and click + ADD. On the TYPE tab of the Instance provisioning wizard, we select the Instance Type to provision. In this case, select "HVM" and click NEXT.

On the GROUP tab, select the Group and Cloud containing the target MVM Cluster and provide a name for the new Instance. In my case, I have an automatic naming policy setting my Instance name, but depending on your appliance configuration you may need to enter a custom name. Click NEXT.

On the CONFIGURE tab, first select the IMAGE. Select the Windows server ISO that was uploaded in the previous step. Based on the minimum memory configuration that was set on the Virtual Image, Plans which are too small will be filtered out. Among compatible Plans, select one that meets your requirements. Next, set the RESOURCE POOL, which is the HVM cluster you're targeting. Configure disks and disk sizes, as well as network details (this will vary based on HVM cluster configuration). Finally, select the HOST, which is the HVM host within the cluster that the new Instance should initially be provisioned onto.

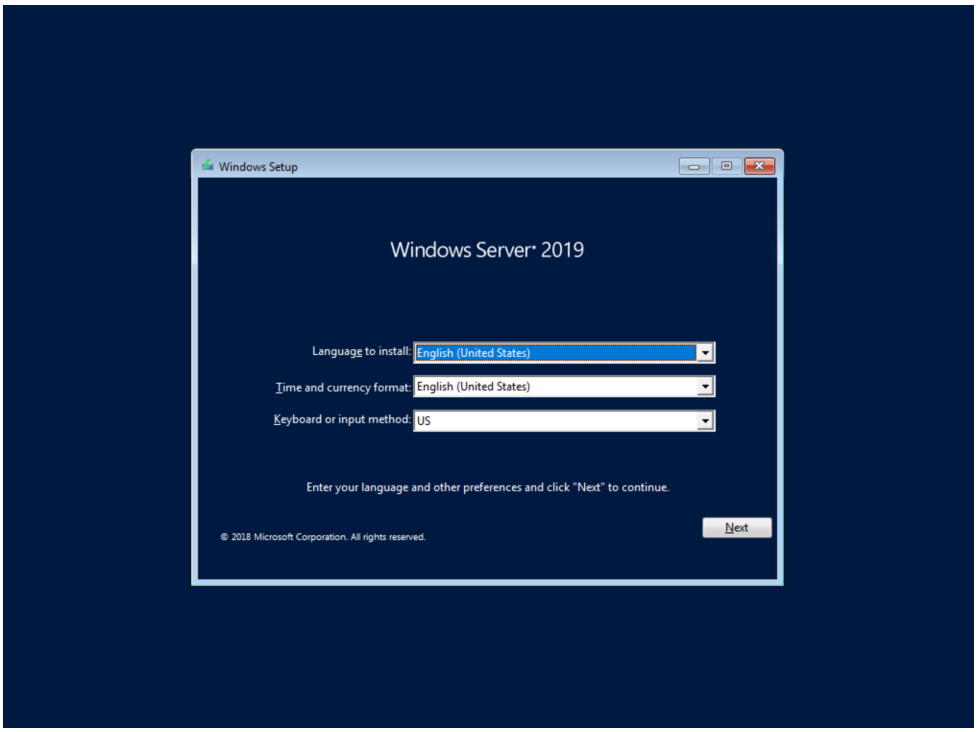
As a final step, we need to also expand the "Advanced Options" section and make sure "ATTACH VIRTIO DRIVERS" is checked. This will attach an ISO containing the VirtIO drivers which we'll use later. Click NEXT.



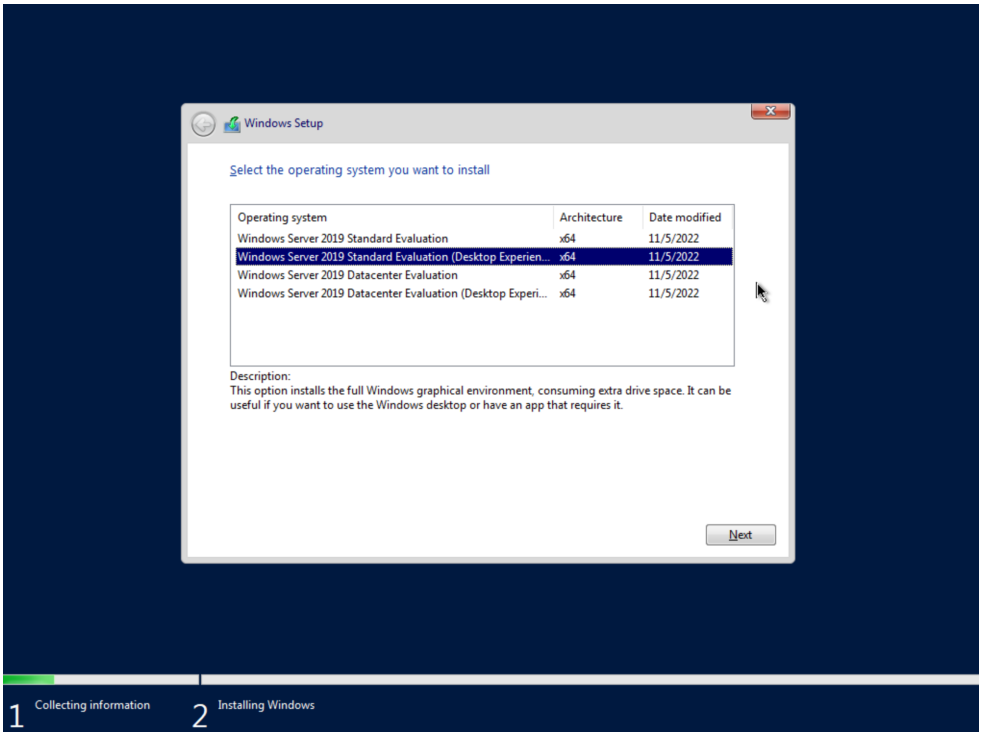
The final two tabs of the wizard, AUTOMATION and REVIEW, do not require any configuration changes though you may want to review the Instance settings on the final tab. When done, click COMPLETE.

Click on the newly provisioning Instance from the Instances list page. Since this image is being provisioned for the first time, the image must be uploaded to the HVM host. This can take a little bit of time but any future attempts to provision workloads from this image will skip this step. Wait for the Instance to fully complete and appear in a green “Ready” status.

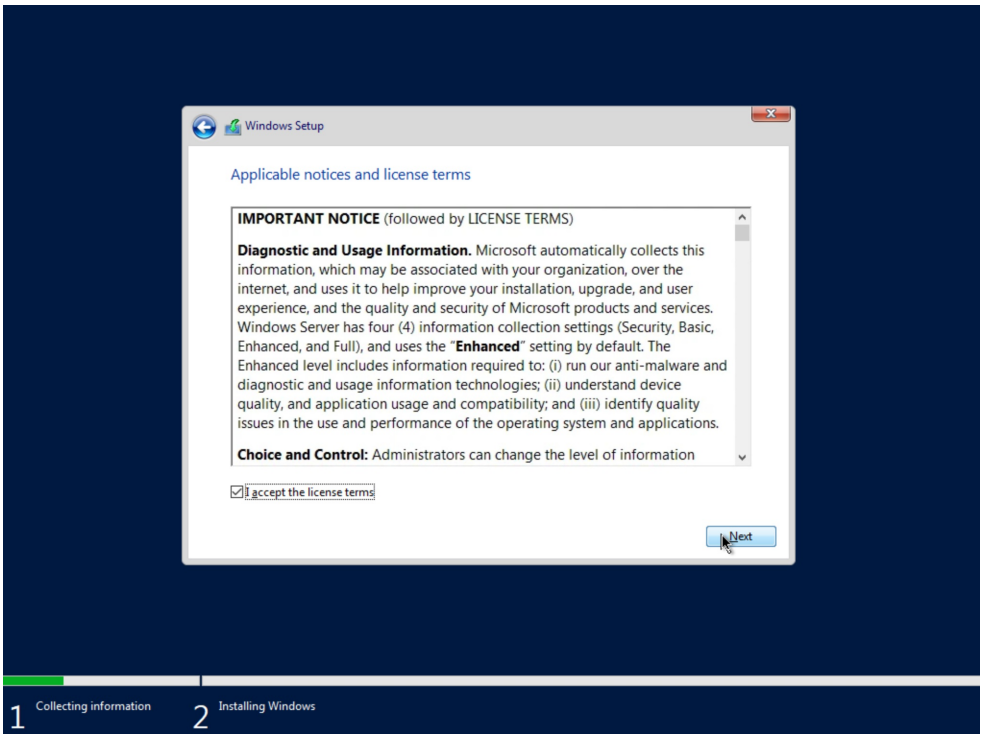
Once the Instance has fully finished provisioning, launch a console session by clicking ACTIONS and then “Open Console.” This will open a new window with a console session into the VM.


Windows Setup
Windows Server 2019
Language to install: English (United States)
Time and currency format: English (United States)
Keyboard or input method: US
Enter your language and other preferences and click "Next" to continue.
© 2018 Microsoft Corporation. All rights reserved.
Next

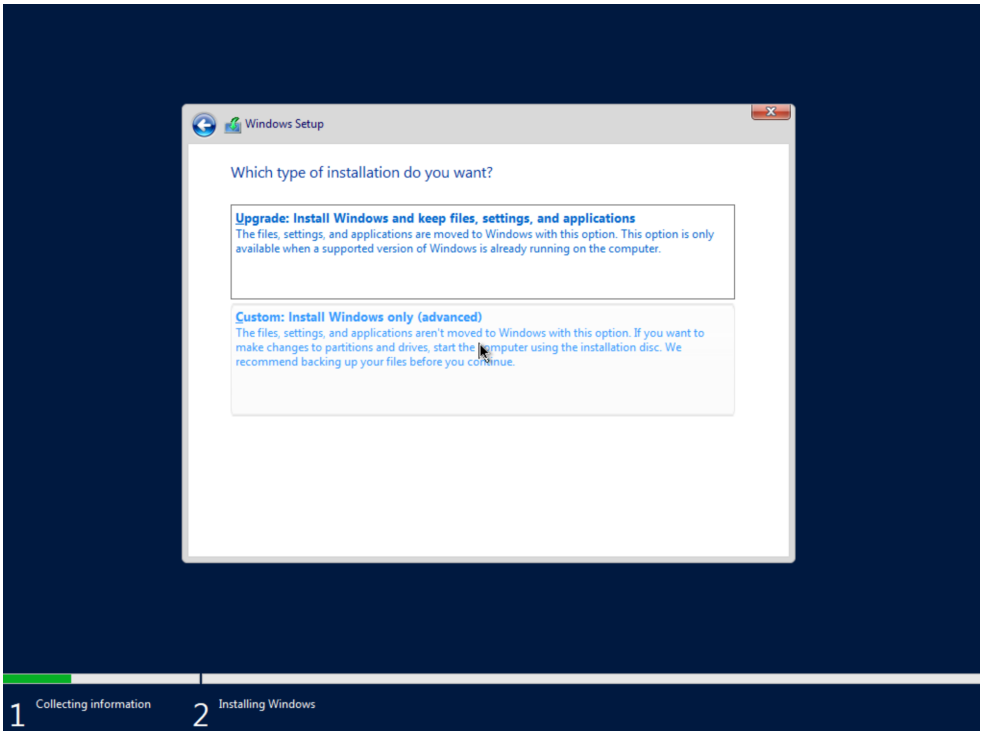
After selecting the language, click “Next.” On the following screen, click “Install Now.” This will begin the Windows setup process on our new VM. You’ll next select the operating system type you wish to install. For this example, I’m installing 2019 standard with desktop experience. Click “Next.”



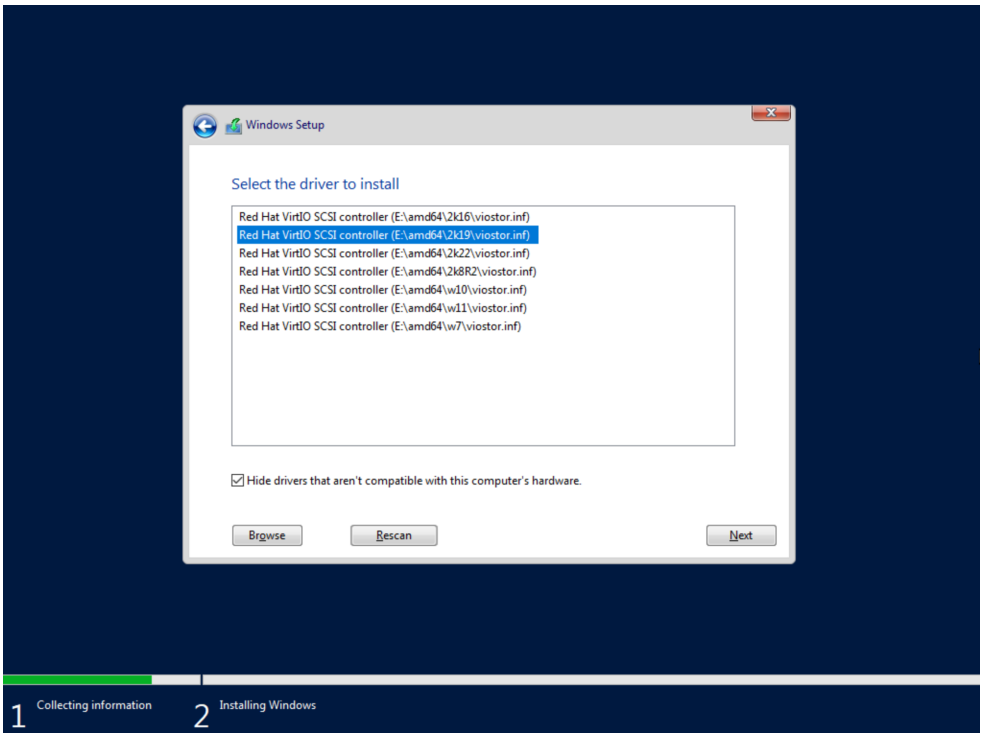
Accept the licensing terms and click “Next.”


Windows Setup
Applicable notices and license terms
IMPORTANT NOTICE (followed by LICENSE TERMS)
Diagnostic and Usage Information. Microsoft automatically collects this information, which may be associated with your organization, over the internet, and uses it to help improve your installation, upgrade, and user experience, and the quality and security of Microsoft products and services. Windows Server has four (4) information collection settings (Security, Basic, Enhanced, and Full), and uses the "Enhanced" setting by default. The Enhanced level includes information required to: (i) run our anti-malware and diagnostic and usage information technologies; (ii) understand device quality, and application usage and compatibility; and (iii) identify quality issues in the use and performance of the operating system and applications.
Choice and Control: Administrators can change the level of information
I accept the license terms
Next
1 Collecting information
2 Installing Windows

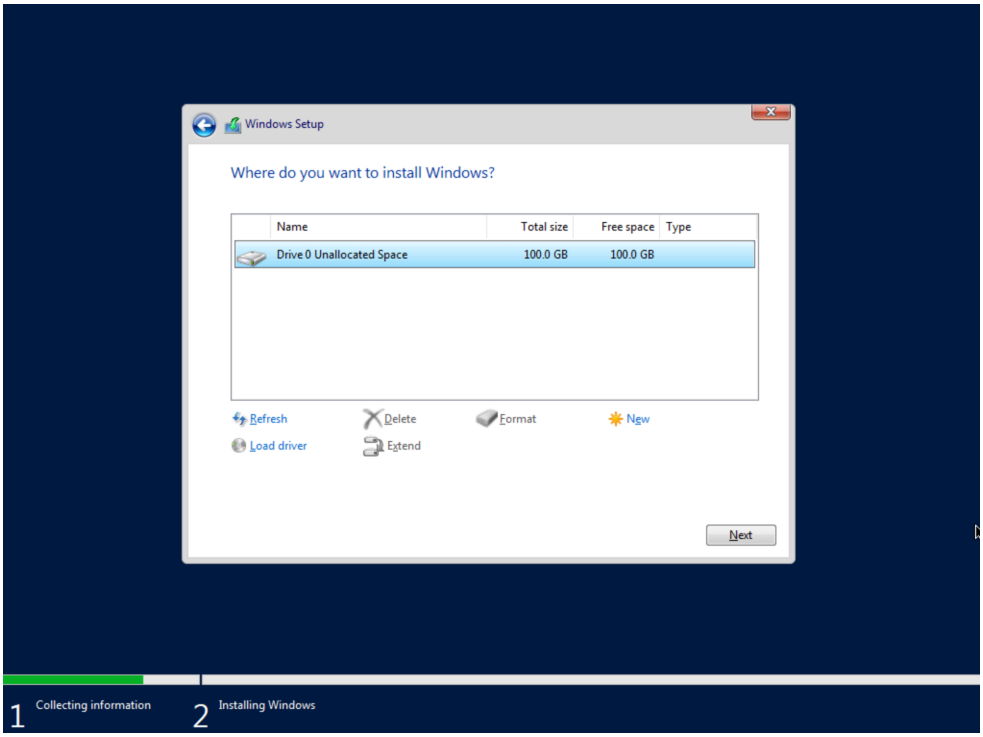
On the next screen, choose a custom install.


Windows Setup
Which type of installation do you want?
Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.
Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.
1 Collecting information
2 Installing Windows

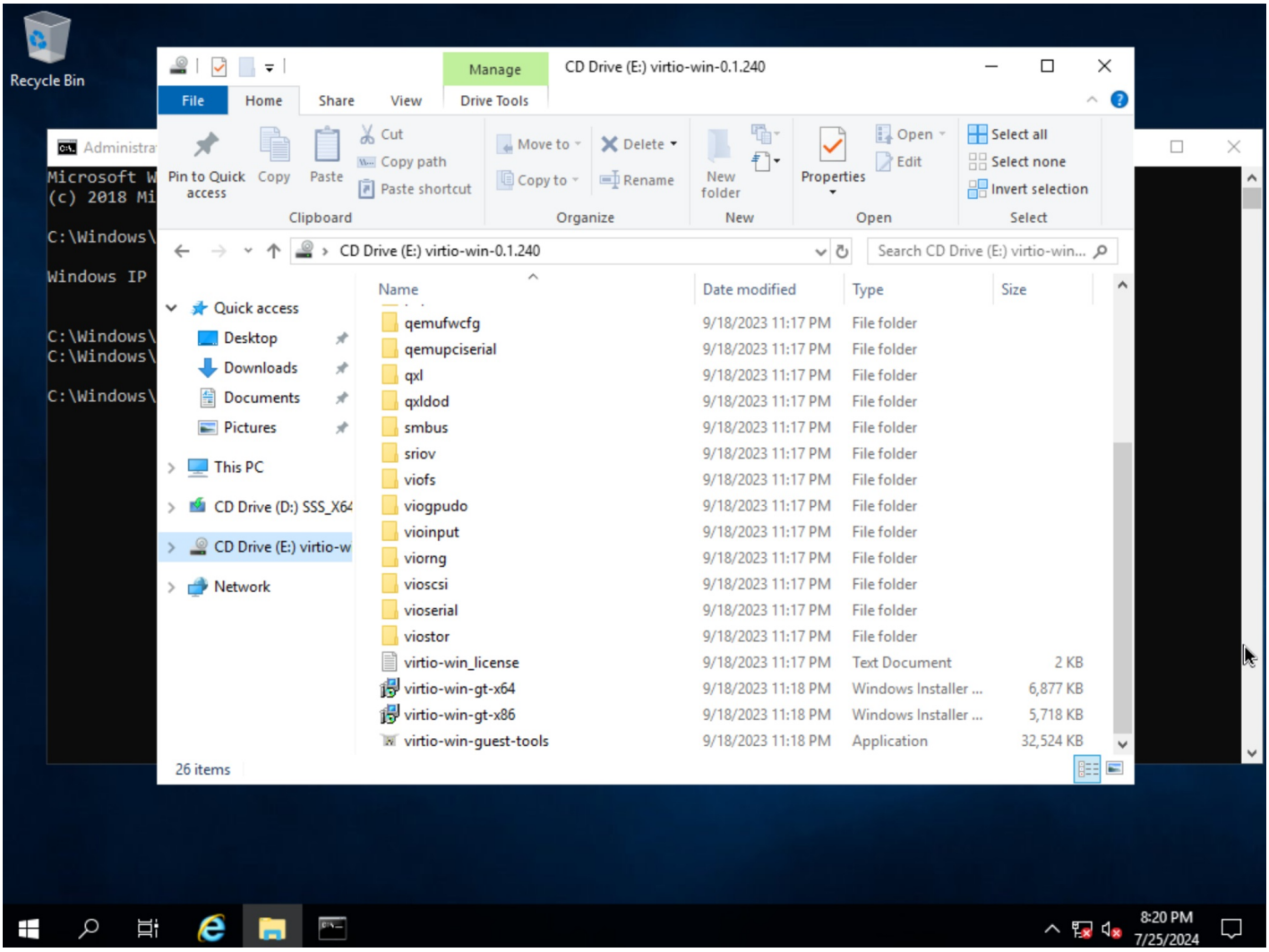
The next screen asks where Windows should be installed and may be empty. Click “Load Driver” to locate the mounted disk image containing the VirtIO drivers. The search should return a number of VirtIO SCSI controller packages for various Windows flavors. Select the proper package for the Windows version being installed. Click “Next.”


Windows Setup
Select the driver to install
Red Hat VirtIO SCSI controller (E:\amd64\2k16\viostor.inf)
Red Hat VirtIO SCSI controller (E:\amd64\2k19\viostor.inf)
Red Hat VirtIO SCSI controller (E:\amd64\2k22\viostor.inf)
Red Hat VirtIO SCSI controller (E:\amd64\2k8R2\viostor.inf)
Red Hat VirtIO SCSI controller (E:\amd64\w10\viostor.inf)
Red Hat VirtIO SCSI controller (E:\amd64\w11\viostor.inf)
Red Hat VirtIO SCSI controller (E:\amd64\w7\viostor.inf)
Hide drivers that aren't compatible with this computer's hardware.
Browse
Rescan
Next
1 Collecting information
2 Installing Windows

After a moment, we’re back at the screen asking where Windows should be installed. We should see the disk(s) of size and type selected at the time the VM was provisioned. Select the proper disk and click “Next.” The Windows installation will now begin. Once Windows has fully installed, proceed to the next step.

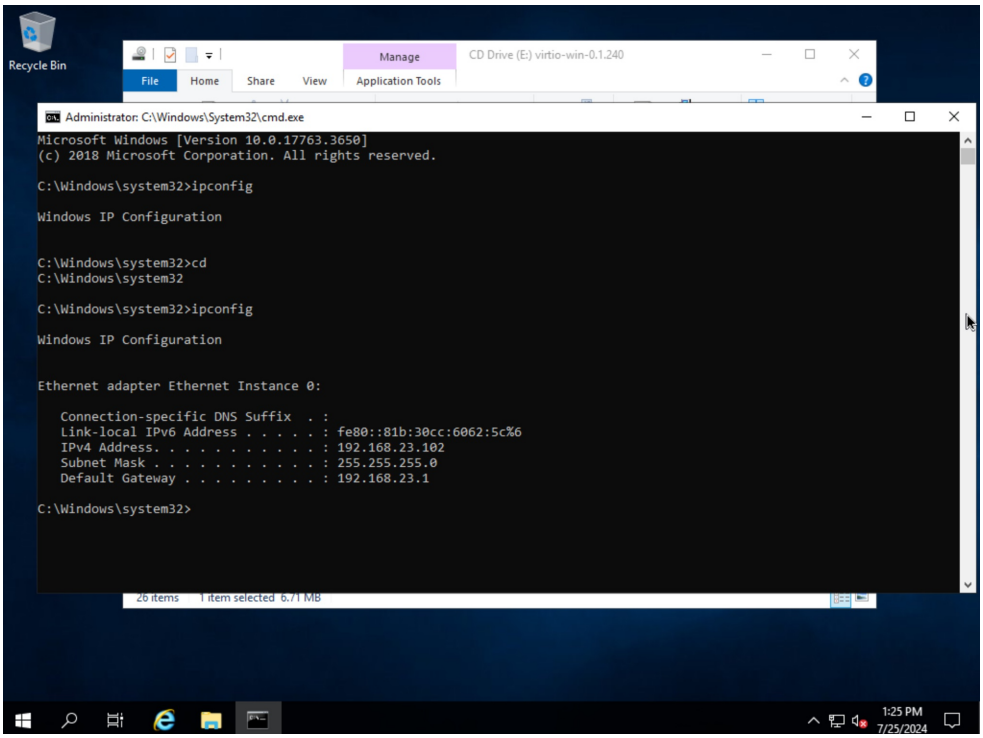


Following installation, Windows will restart and prompt for an Administrator user password. Set the password and log in as Administrator. Currently, there are no network interfaces configured. We need to install the VirtIO drivers to get this machine onto the network. We have a disk image mounted with the driver installer so we need to navigate to that drive and launch the installer. Open Windows Explorer and locate the drive in the side bar. In my case, it's the E: drive. Right-click on `virtio-win-guest-tools` and select "Install."

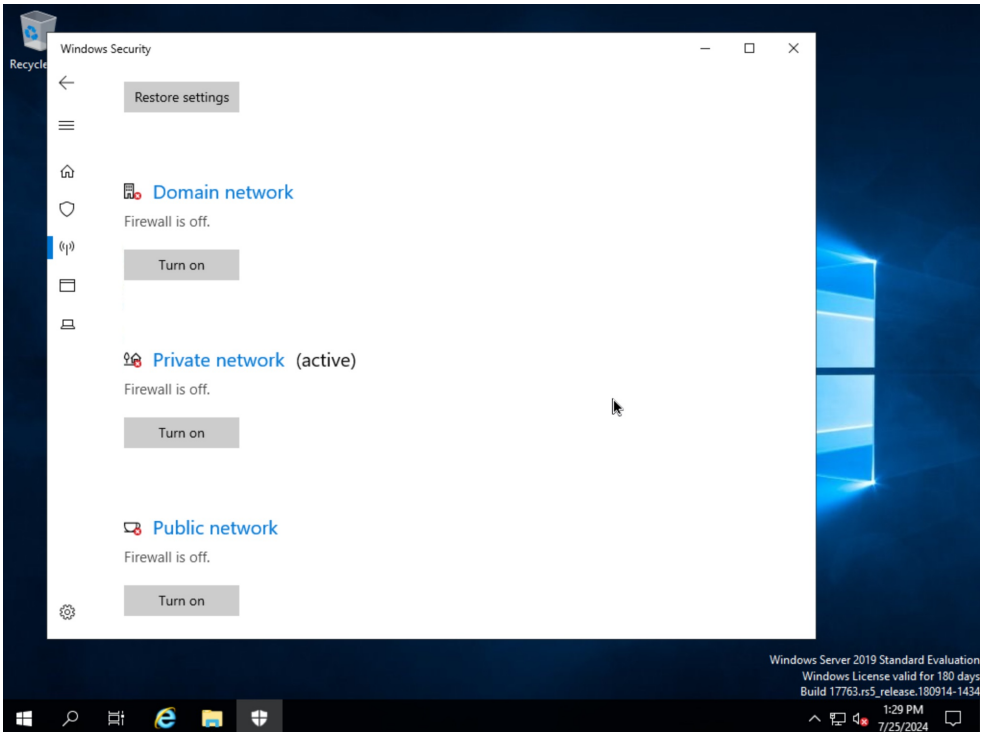


Step through the installer. Simply click "Next" or "Install" through each step, there are no configuration changes needed. Once the installer

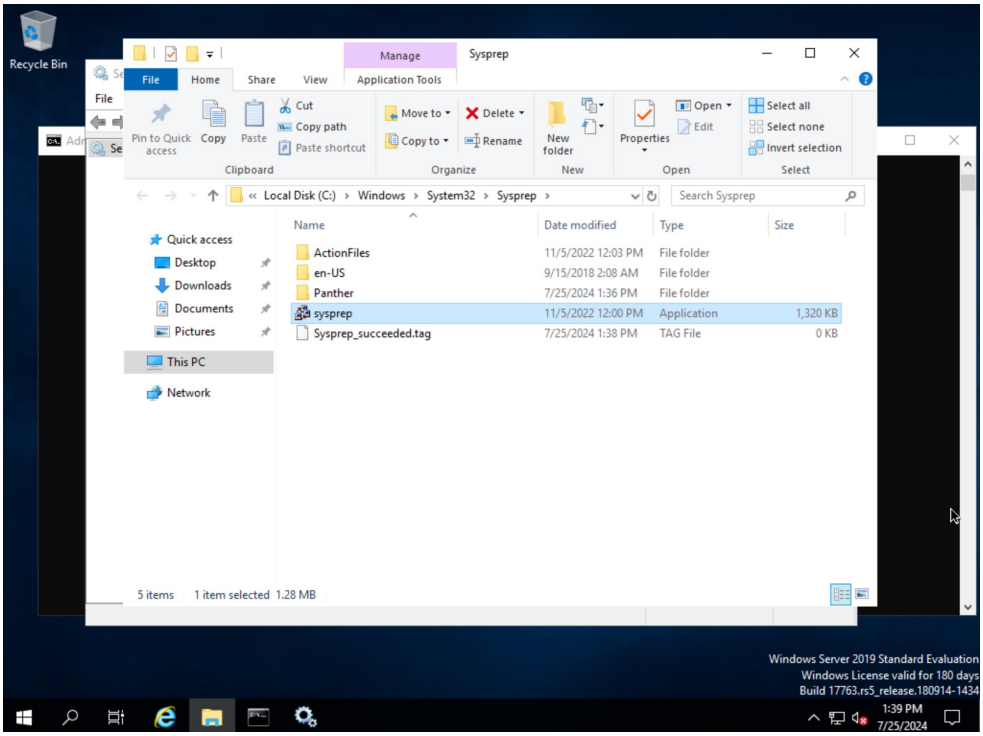
has completed, click “Finish.” You can confirm we now have a network interface by opening a Command Prompt session and using the `ipconfig` command. One network adapter should be listed.



We can now eject the two virtual disks, drives D: and E: in my case. Then, launch Windows Security so we can disable firewalls. Turn off firewall for domain, private network, and public network.



Next, back in Command Prompt, run `winrm quickconfig` to configure `winrm`. Within `Services`, ensure that `winrm` (Windows Remote Management) is set to automatic on startup. Right-click on the Start button and select Run. Enter “sysprep” and click OK. In the Windows Explorer window that appears, right-click on `sysprep` and click “Run as Administrator”. Under “Shutdown Options”, choose Quit and click OK. If this is set to shutdown, VM Essentials will simply restart the VM. Once this is completed, a new file `Sysprep_succeeded.tag` appears in Windows Explorer.



We're now done configuring Windows and the console window can be closed. We'll move on to creating a template from the VM we just configured. Begin by opening an SSH session into the VM Essentials appliance server. Confirm `jq` is up to date on the appliance box (`apt install jq`). Then, go ahead and stop the running Windows VM. We can do this from the Instance detail page in VM Essentials. Click ACTIONS and then "Stop Server." Still on the Instance detail page, click ACTIONS and then "Import as Image." This will perform a snapshot and create a new Virtual Image (Library > Virtual Images).

The Virtual Image is not usable until it's in an active status and the UI indication may display an active status even before it's fully ready. If it's "SAVING" or "QUEUED," it is still being prepared and saved. To determine the current status of the Virtual Image, check with a call to VM Essentials API like the one below. When the return output lists a status of "Active," the image is ready to be provisioned from.

```
curl -k --request GET --url https://xx.xx.xx.xx/api/virtual-images/<id>
--header 'accept: application/json' --header 'authorization: Bearer xxx-xxx-xxx-xxx-
xxx' |
jq '.virtualImage.status'
```

Once saved, additional configurations are needed on the Virtual Image in VM Essentials. Edit the new Virtual Image and check the following configurations:

- **MINIMUM MEMORY:** Set as appropriate
- **SYSPREPPED/GENERALIZED IMAGE?:** Checked
- **INSTALL AGENT?:** Checked
- **USERNAME:** Remove if present
- **PASSWORD:** Remove if present
- **VIRTIO DRIVERS LOADED?:** Checked

All other checkbox-type configurations not mentioned in the above list should be unchecked. Click SAVE CHANGES.

At this point all image preparation steps are completed. Repeat the process of provisioning an HVM Instance Type selecting the new image in the future when needed.

Utilizing Existing QCOW Images from an NFS File Share

Integrated NFS shares can be used both as a repository for HVM cluster images and as a target for saving new images from existing VMs. This offers benefits of greatly expanding the available storage compared to what's available on the VM Essentials manager VM, insulates you from issues that can arise from images completely filling the manager storage, and allows for the same images to be easily integrated

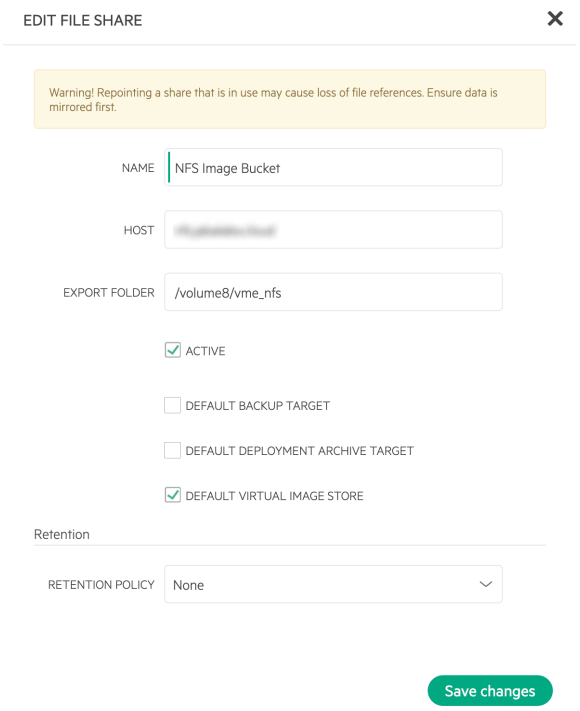
with multiple VM Essentials appliances.

To begin, we need the NFS file share integrated with VM Essentials. This is done in the Infrastructure > Storage section of the UI. This guide assumes the NFS file share is pre-existing and the VM Essentials manager can reach it. Actually setting up an NFS file share goes beyond the scope of this guide. From the File Shares tab, check to see the desired file share is already integrated. If needed, you can add one by clicking + ADD and then selecting “NFSv3”.

When adding a new file share, configure the following:

- **NAME:** A friendly name for the file share within VM Essentials
- **HOST:** The IP address or hostname for the NFS file share server
- **EXPORT FOLDER:** The path to the folder that should be mounted to the manager
- **ACTIVE:** Must be checked to be able to consume this file share elsewhere in VM Essentials manager UI
- **DEFAULT VIRTUAL IMAGE STORE:** (Optional) Select if you wish this file share to be the default store for newly uploaded or generated images

When done, click Save changes.



IMPORTANT

You must configure the NFS share to give VM Essentials manager read and write access if you want to be able to read images from and write images to the file share. Configuring NFS file shares goes beyond the scope of this guide. Deleting files from an integrated file share deletes the actual file and not just the representation of the file in VM Essentials. This includes Virtual Images. Deleting a Virtual Image that is backed by a QCOW image file stored in an integrated file share will also cause the file itself to be deleted in addition to the Virtual Image object within VM Essentials.

With the file share integrated, we can now create Virtual Images which are backed by QCOW images that are pre-existing in the file share. Navigate to Library > Virtual Images and click + ADD. From the dropdown, select “QCOW2”. Make the configurations specified below. Those not mentioned can often be left on the default value. For a deeper explanation of configurations not mentioned here, see the dedicated section of VM Essentials documentation on Virtual Images.

- **NAME:** A friendly name for the image in VM Essentials
- **OPERATING SYSTEM:** Specify the operating system of the image
- **MINIMUM MEMORY:** Enter a minimum memory value and VM Essentials will not allow the image to be provisioned using a plan with lower memory

- **BUCKET:** Select the NFS share integrated in the previous step
- **CREATE IMAGE ID:** Set to “URL/PATH”
- **URL:** Enter the path to the QCOW image within the file share. See the next paragraph for a deeper explanation of how to enter the path properly

The entered path to the QCOW image should not include the name of the NFS share or the name of the file itself. See the portion highlighted in the screenshot:

It also should only be the path to the folder containing the QCOW image. The file name itself should not be part of the path. For example, `templates/qcow/ubuntu/server/2204/011025`. Click Save changes.

With the NFS file share integrated and the Virtual Image created, the image is now usable from the provisioning wizard. This guide won’t fully cover the use of the provisioning wizard but from the Configure tab of the wizard, the image is now selectable (assuming you’ve selected a compatible provisioning target). Additionally, we can now click into the detail page for running Instances and save them to images backed by the NFS file share. From the Instance detail page, click Actions, then “Import as Image.” You’ll be able to set a name for the new image and specify the NFS file share as the target bucket.

Hardware Passthrough

HPE Morpheus VM Essentials includes hardware passthrough and pooling support for VMs provisioned to HVM Clusters. This support extends to GPU, USB and NVME devices. In order to be usable, such devices must be attached to a HVM Host or to multiple HVM Hosts. HPE Morpheus VM Essentials includes controls to detach hardware devices from the underlying OS on the hypervisor host and add them to a pool where they are available for consumption by VMs. GPU hardware can be attached to VMs at provision time through custom Service Plans or on an ad-hoc basis by manually attaching hardware to existing VMs. Other supported hardware types must be passed through to the VM after provisioning.

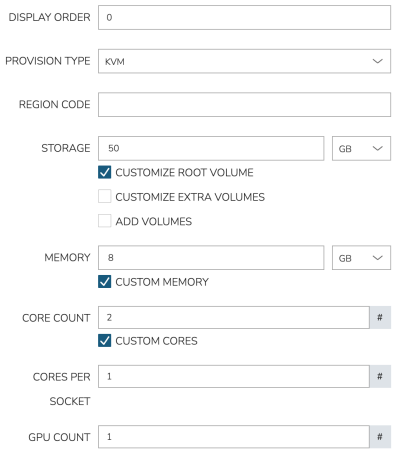
Subtopics

Creating Service Plans
Viewing and Assigning Hardware Devices
GPU Passthrough Example

Creating Service Plans

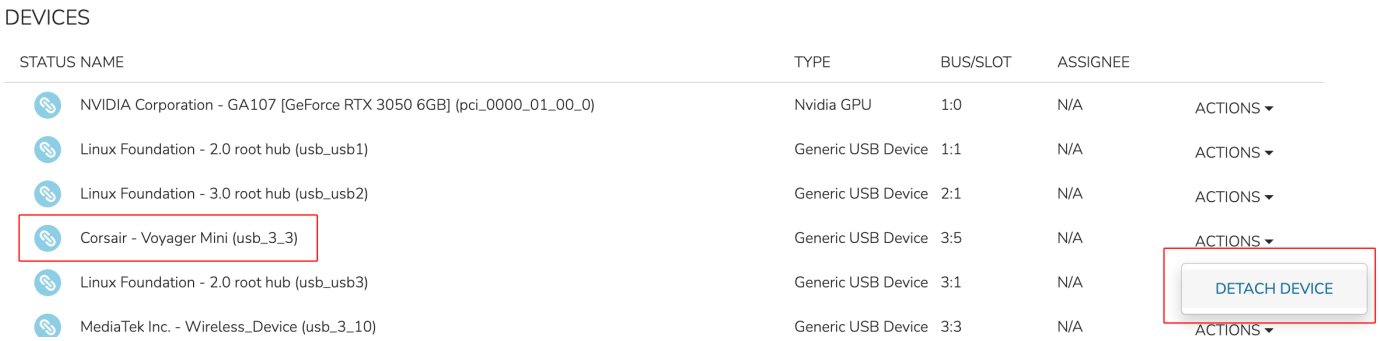
When utilizing GPU hardware, it may be most convenient to use a custom Service Plan. This allows administrators to pre-configure the number of discrete hardware cards to attach to the VM at provision time. Once provisioned, the specified number of GPUs will be attached to the VM. For workloads which are provisioned and torn down regularly, this will save additional steps of manually attaching GPUs available from the pool. On teardown, attached devices of all types are released back to the pool. Though in some cases utilizing Service Plans may be most convenient, as you’ll see in the next sections it is not strictly required. It is also possible to manually attach GPUs or other hardware types on any existing VMs running on the HVM Cluster.

To create a new Service Plan, navigate to Administration > Plans. Click + Add and then Service Plan. In the New Service Plan modal, first set the PROVISION TYPE configuration to “KVM.” This will update the available configuration fields and reveal the GPU COUNT configuration. Use this configuration to set the number of GPU hardware cards which should be attached to provisioned VMs using this Service Plan. All other configuration fields for Service Plans go beyond the scope of this section. When finished, click SAVE CHANGES.

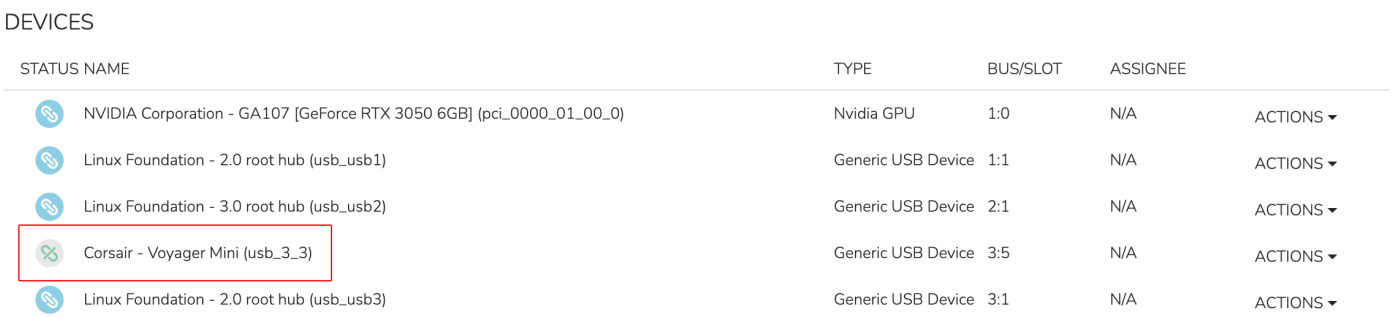


Viewing and Assigning Hardware Devices

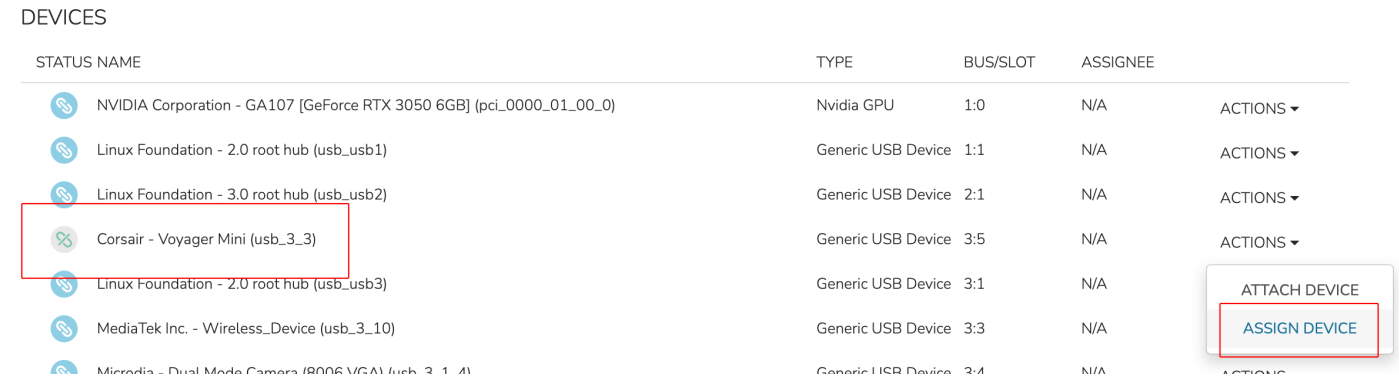
Hardware Devices are surfaced at the Host detail level and the VM (server) detail level through a Devices tab. The Host detail will show all attached hardware devices and their current status: Attached (to the host), detached (from the host), or assigned (to a VM). The VM detail will show only hardware devices currently attached to that VM. To begin consuming hardware devices with HVM Cluster VMs, look again at the list in the Devices tab on the Host detail page. Detach a piece of hardware from the host using the ACTIONS dropdown for that piece of hardware. As shown in the screenshot below, DETACH DEVICE is selected for a USB device.



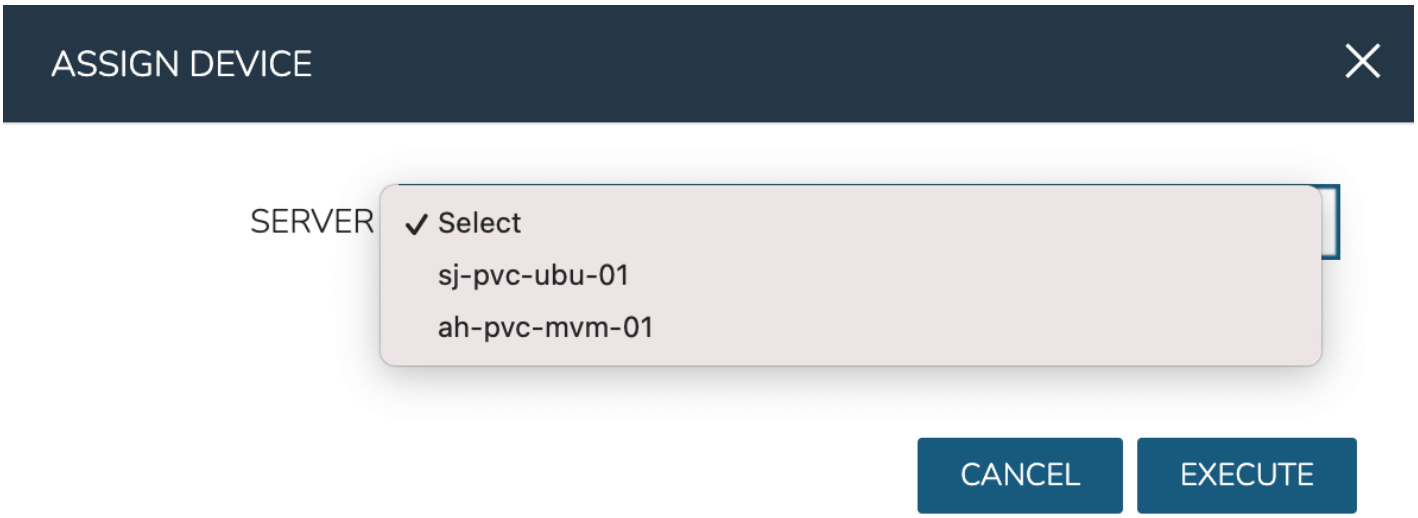
Once detached, the status of the device is changed to “Detached” (see screenshot below) and the device is available for consumption by VMs running on this host.



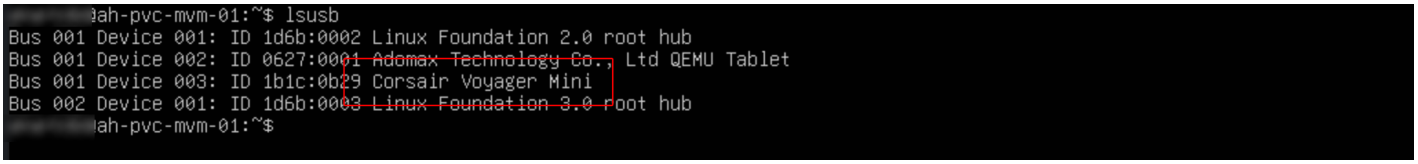
To assign the hardware to a specific VM, click the ACTIONS dropdown once again for the now-detached hardware. Now, click ASSIGN DEVICE.



Within the ASSIGN DEVICE modal that will appear, select the server for device assignment and click EXECUTE.



The icon and status for the device in the hardware list has now changed to "Assigned." If we then open a console session with this VM, we can see the USB device is assigned successfully and is usable by the guest OS.


ah-pvc-mvm-01:~$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 0627:0001 Adomax Technology Co., Ltd QEMU Tablet
Bus 001 Device 003: ID 1b1c:0b29 Corsair Voyager Mini
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
ah-pvc-mvm-01:~$

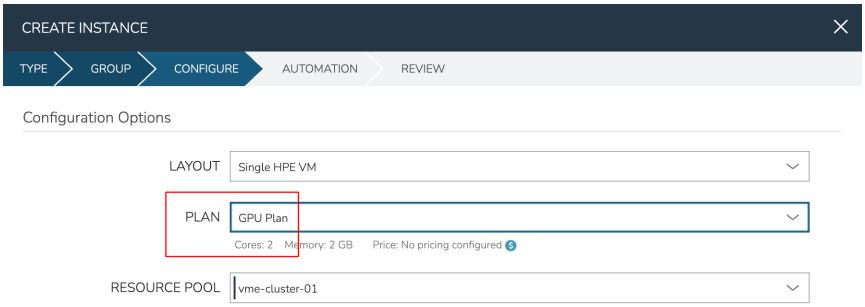
The same process can be used to detach and assign GPU or NVME devices.

GPU Passthrough Example

In a previous section, a Service Plan was created which consumes a GPU when a VM is provisioned using that Plan. This section shows an example provisioning a workload using that Plan and a GPU-accelerated workload running on the VM. In this example, there is an Nvidia GeForce RTX 3050 connected to one of the HVM Hosts. By passing the GPU hardware through to a provisioned VM, hardware-accelerated AI workloads can be run on the VM.

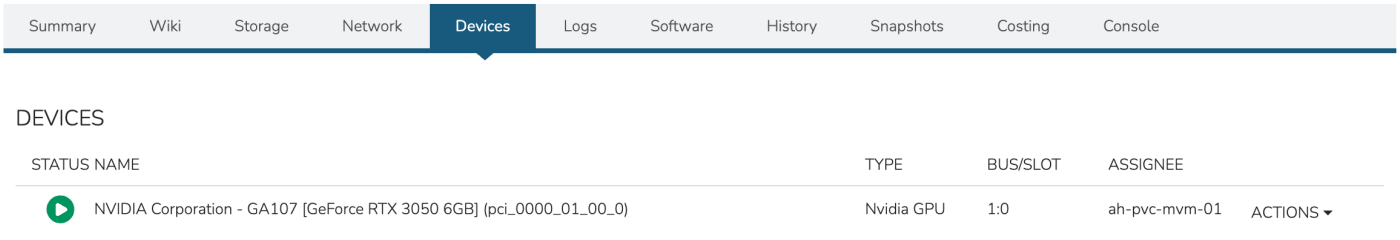
Begin by navigating to Provisioning > Instances. The list of all currently-managed Instances is here along with high level information (power state, etc). To begin a new Instance, click + ADD. Choose type HVM and click NEXT. On the next pane, choose the Group and Cloud in which your desired HVM Cluster resides, name the Instance, and click NEXT.

On the CONFIGURE tab, the main thing to note for this example is the PLAN configuration. This dropdown contains some default Plans that are included with HPE Morpheus VM Essentials and compatible with the HVM provisioning technology (named "1 CPU, 1GB Memory", etc). This dropdown also includes user-created Plans, such as those you've created to consume GPU hardware. In the screenshot below, you can see the "GPU Plan" was selected.



From here, complete the Instance provisioning wizard selecting any automation or lifecycle configurations and wait for the Instance provisioning to complete.

With provisioning complete, check the attached device(s) from the HPE Morpheus VM Essentials UI. This is done from the VM level rather than the Instance level. From the Instance detail page, click on the Resources tab. Click on the name of the desired VM to access the VM detail page. Click on the Devices tab. As in the screenshot below, the attached GPU should be shown.



To go further, open a console session to the new VM either through HPE Morpheus VM Essentials UI or by connecting to the VM over SSH from a local terminal session. Use the `lspci` command to view all devices connected to PCI buses. The attached GPU should be shown here as it is in the UI.

At this point, the VM is ready to run GPU-accelerated workloads normally. To test this, I'll run Ollama which is an open-source tool designed to make it easy to run large language models (LLMs) locally. In the screenshot below, see the AI chatbot response to an input. This result took only a few seconds thanks to GPU hardware acceleration.

```
ahark86@ah-pvc-mvm-01:~$ ollama run llama2
>>> tell me about hpe

Hewlett Packard Enterprise (HPE) is a leading technology company that provides a wide range of products, services, and
solutions to businesses, organizations, and governments around the world. Here are some key things to know about HPE:

1. History: HPE was formed in 2015 as a result of the merger between Hewlett-Packard (HP) and Enterprise Services, a
subsidiary of Dell. The company has a long history dating back to 1939 when William Redington Hewlett and David Packard
founded HP in a small garage in Palo Alto, California.
2. Business segments: HPE operates through two main business segments: Enterprise Group and Technology Services. The
Enterprise Group provides hardware, software, and services to help customers build, manage, and secure their IT
infrastructures. The Technology Services segment offers a range of services, including cloud computing, application
management, and cybersecurity.
3. Products and services: HPE offers a wide range of products and services, including servers, storage devices, networking
equipment, software, and services. Some of its popular products include the ProLiant server, the 3PAR storage array, and
the Aruba networking portfolio.
4. Cloud computing: HPE is a leading provider of cloud computing solutions, offering a range of services and tools to help
customers build and manage their own clouds, as well as consume cloud services from HPE. The company's cloud offerings
include HPE Helion Managed Cloud Services, HPE Helion Cloud Platform, and HPE Helion Development Platform.
5. Artificial intelligence (AI) and machine learning (ML): HPE is a pioneer in the field of AI and ML, with a range of
solutions and services designed to help customers leverage these technologies to improve their business outcomes. The
company's AI and ML offerings include the HPE Ezmeral AI Platform, HPE Machine Learning Studio, and HPE Vertica for AI and
ML workloads.
6. Cybersecurity: HPE is a leading provider of cybersecurity solutions, offering a range of products and services designed
to help customers protect their IT infrastructures from cyber threats. The company's cybersecurity offerings include the
HPE Aruba ClearPass security management platform, the HPE Aruba NetProtect network security solution, and the HPE Fortify
on Demand application security service.
7. Partnerships and collaborations: HPE has a strong track record of forming partnerships and collaborations with other
technology companies to deliver joint solutions and services to customers. Some of its key partners include Microsoft,
Cisco, and SAP.
8. Locations: HPE has operations in over 170 countries around the world, with major locations in North America, Europe,
Asia, and Australia. The company's global headquarters is located in San Jose, California.
9. Employment: HPE employs over 50,000 people worldwide, with a diverse range of roles including engineering, sales,
marketing, and support. The company offers a range of career development opportunities and programs to help employees grow
and succeed.
10. Community involvement: HPE is committed to giving back to the communities where it operates, with a focus on
education, innovation, and social responsibility. The company supports a range of charitable organizations and initiatives
around the world.

>>> Send a message (/? for help)
```

With the request completed, we can run the `ollama ps` command which confirms the model was running under GPU acceleration.

```
ahark86@ah-pvc-mvm-01:~$ ollama ps
NAME            ID              SIZE      PROCESSOR    UNTIL
llama2:latest    78e26419b446    5.6 GB    100% GPU     4 minutes from now
```

Network

Subtopics

- Networks
- Network Groups
- Routers
- IP Pools
- Floating IPs
- Domains
- Proxies
- Integrations

Networks

Infrastructure > Network > Networks

Subtopics

- Overview
- Configuring Networks

Overview

The Networks section is for configuring networks across all Clouds in VM Essentials. Existing networks from Clouds added in VM Essentials will auto-populate in the Networks section.

Networks can be configured for DHCP or Static IP assignment, assigned IP pools, and configured for visibility and account assignment for multi-tenancy usage. Inactive Networks are unavailable for provisioning use. In addition, VM Essentials allows administrators to restrict management of VM Essentials-created Networks through Role permissions.

Configuring Networks

Subtopics

- DHCP
- Static and IP Pools
- Advanced Options (Search Domains)
- Group and Tenant Access
- Guest Console SSH Tunnel
- Subnets

DHCP

About this task

To configure a network for DHCP:

Procedure

1. Navigate to Infrastructure > Network > Networks
2. Search for the target network
3. Edit the Network by either:
   - Select Actions > Edit
   - Select the Network, then select Edit
4. In the Network Config modal, set the DHCP flag as Active (default)
5. Save Changes

Results

IMPORTANT

The DHCP flag tells VM Essentials this network has a DHCP server assigning IP Addresses to hosts. VM Essentials does not act as the DHCP server, and provisioning to a network that has the DHCP server flag active in VM Essentials, but no DHCP server actually on the network will, in most cases, cause the instance to not receive an IP address.

NOTE

When selecting a network with DHCP enabled during provisioning, “DHCP” will populate to the right of the selected network:

Static and IP Pools

About this task

To configure a network for Static IP Assignment:

Procedure

1. Navigate to Infrastructure > Network > Networks
2. Search for the target network
3. Edit the Network by either:
   - Select Actions > Edit
   - Select the Network, then select Edit
4. In the Network Config modal, add the following:
   - Gateway
   - DNS Primary
   - DNS Secondary
   - CIDR ex 10.10.10.0/22

- VLAN ID (if necessary)
- Network Pool * Leave as “choose a pool” for entering a static IP while provisioning * Select a Pool to use a pre-configured VM Essentials or IPAM Integration IP Pool
- The Permissions settings are used for Multi-Tenant resource configuration
  - Leave settings as default if used in a single-tenant environment (only one Tenant in your VM Essentials appliance)
  - To share this network across all accounts in a multi-tenant environment, select the Master Tenant and set the Visibility to Public
  - To assign this network to be used by only one account in a multi-tenant environment, select the account and set visibility to Private
- Active
  - Leave as enabled to use this network
  - Disable the active flag to remove this network from available network options

5. Save Changes

Results

NOTE
When selecting a network with DHCP disabled and no IP Pool assigned during provisioning, an IP entry field will populate to the right of the selected network(s):

NOTE
When selecting a network with an IP Pool assigned during provisioning, the name of the IP pool will populate to the right of the selected network(s). IP Pools override DHCP.

Advanced Options (Search Domains)

Search domains are appended to DNS searches when a **non** fully qualified domain name (short name) is queried. Search domains can be entered as comma separated values, which will be added to DNS configurations, such as /etc/resolv.conf These domains are injected via cloud-init or other method chosen for the virtual image.

Group and Tenant Access

Networks can be configured to provide specific Group access, if desired. **Group Access** controls which Groups at provision time will have access to the Network resource. Only workloads being provisioned to the selected Groups would have visibility into the Network. Workloads provisioned to other Groups would not see the Network as an available selection.

Guest Console SSH Tunnel

In some scenarios, Instances that are segregated from the VM Essentials appliance by port restrictions, or other mechanisms, can cause difficulties to access the guest console via the VM Essentials web UI. Guest Console SSH Tunnel settings allow the administrator to configure a jump host’s settings that is dual-homed, accessible by VM Essentials but also resides on the segregated network. When the guest console is configured with the SSH protocol, the traffic will be routed to the jump host, which will then relay to the target instance.

GUEST CONSOLE JUMP HOST

DNS hostname or IP of the jump host to relay the traffic

GUEST CONSOLE JUMP PORT

Port override, if different than 22 for SSH

GUEST CONSOLE JUMP USERNAME

Username used to authenticate to the jump host

GUEST CONSOLE JUMP PASSWORD

Password that is used with the username to autenticate to the jump host

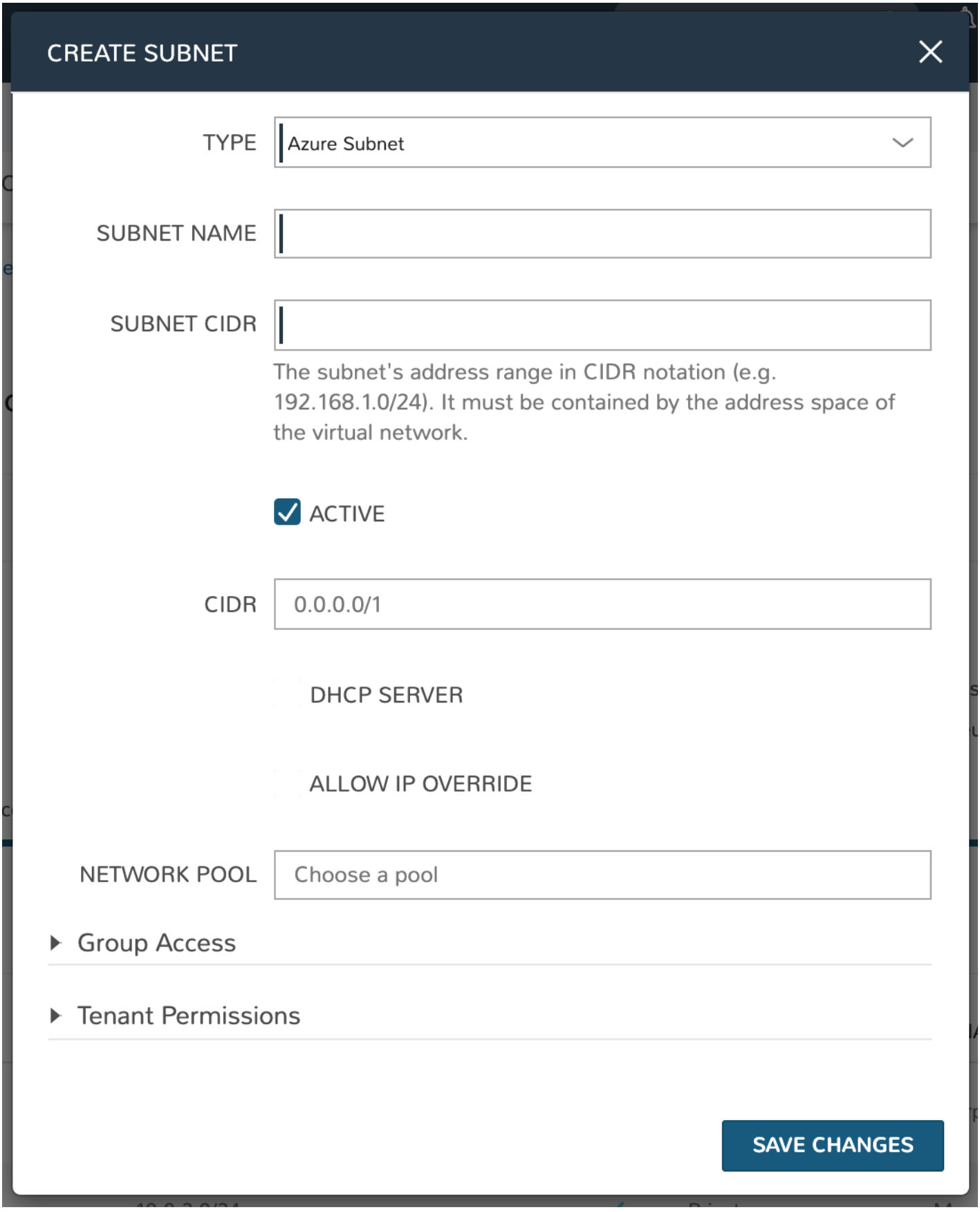
GUEST CONSOLE KEYPAIR

Keypair saved in VM Essentials to be used in lieu of, or in addition to, the password to the jump host, which is associated with the configured username Keypairs can be imported at: Infrastructure > Trust > Key Pairs

Subnets

Subnet details can be viewed from the SUBNETS tab on the detail page of a specific network. From the SUBNETS tab, Morpheus allows the user to search and edit existing subnets.

In an Azure VNet, you can also create new subnets with the +ADD button.



Network Groups

Network Groups are useful for grouping networks during provisioning and scaling or grouping availability subnets together such that during provisioning vm's within an instance can be round robin provisioned across availability zones.

Subtopics

Adding Network Groups

Adding Network Groups

Procedure

1. Navigate to Infrastructure > Network > Networks Groups
2. Select ADD
3. Enter the following:

   Group info:

   - *Name*: Name of the Network Group in VM Essentials
   - *Description*: Details of the Network Group in VM Essentials

   Networks

   - Search for and select target Networks for the Network Group
   - Search for and select target Subnets for the Network Group

   Group Access

   - Set Group Access for the Network Group. Group access controls which Groups at provision time will have access to this resource. Select "all" (default) to give workloads provisioned to any Group access to this resource. If this resource should be restricted only to workloads provisioned to specific Groups, select all that apply.
4. Select SAVE CHANGES

Routers

Subtopics

Overview
Create New Router
Editing Existing Routers
Deleting Existing Routers

Overview

Routers can be viewed, created, and managed from the Routers tab of the Infrastructure > Networks page. VM Essentials supports the creation of the following router types depending on networks that are currently configured:

- OVS Bridge Domain

Create New Router

Procedure

1. Navigate to Infrastructure > Networks > Routerstab
2. Click + ADD
3. Select the router type and complete the fields on the resulting modal
4. Once complete, click ADD NETWORK ROUTER

Editing Existing Routers

Procedure

1. Navigate to Infrastructure > Networks > Routerstab
2. Click on the pencil icon for the appropriate router
3. After editing router fields, click SAVE

Deleting Existing Routers

Procedure

1. Navigate to Infrastructure > Networks > Routerstab
2. Click on the trash can icon for the appropriate router
3. Acknowledge the pop-up banner ensuring you wish to delete the router

IP Pools

Infrastructure > Network > IP Pools

Subtopics

Overview
To add a VM Essentials Network Pool

Overview

The IP Pools tab in the Networks section allows you to create HVM-type IP Pools (which is an IP address range VM Essentials can use to assign available static IP addresses to Instances) and NSX IP Pools. The IP Pool section also displays pools synced from IPAM integrations like Infoblox, Bluecat and others.

To add a VM Essentials Network Pool

To add a VM Essentials Network Pool

Procedure

1. Click + ADD in Infrastructure > Network > IP Pools
2. Enter the following:

   Name

   A friendly name for the IP Pool in VM Essentials.

   Pool Type

   Currently, HVM-type IP Pools and NSX IP Pools (with a configured integration) can be created directly from VM Essentials

   Starting Address

   The starting IP address of the IP Pool address range. ex: 192.168.0.2

   Ending Address:

   The ending IP address of the IP Pool address range. ex: 192.168.0.255
3. Save Changes

Results

NOTE
Multiple Address Ranges can be added to a pool by selecting the + icon next to the address range.

After saving the IP pool will be available for assignment to networks in the NETWORK POOL dropdown when adding or editing a network.

Floating IPs

Subtopics

Overview
Floating IPs List Page
Working with Floating IPs

Overview

VM Essentials supports sync and management of floating IP addresses for OpenStack, Huawei, and OTC Clouds. When these Clouds are integrated and floating IPs are present, VM Essentials will automatically sync them in. Once synced, floating IPs are viewable from their own list page (Infrastructure > Network > Floating IPs) and related options are presented during provisioning, teardown, and from Instance detail pages.

NOTE
The Floating IPs tab is present only when supported Clouds are integrated and floating IPs are available. Additional Cloud support is planned for the future.

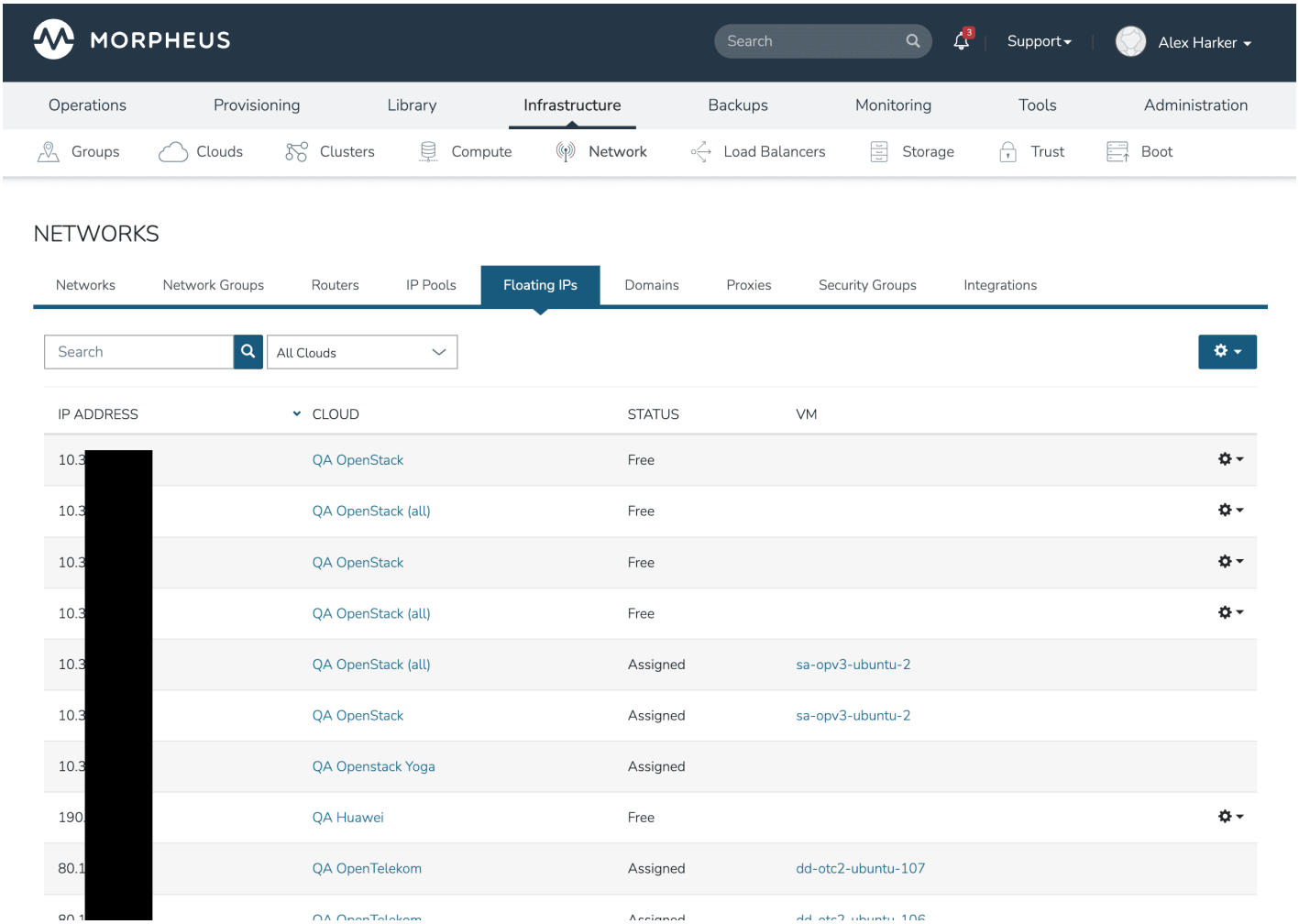
Floating IPs List Page

Floating IPs List Page

All Floating IPs known to VM Essentials can be viewed on the Floating IPs List Page (Infrastructure > Network > Floating IPs). From the Floating IPs list page we can see the following:

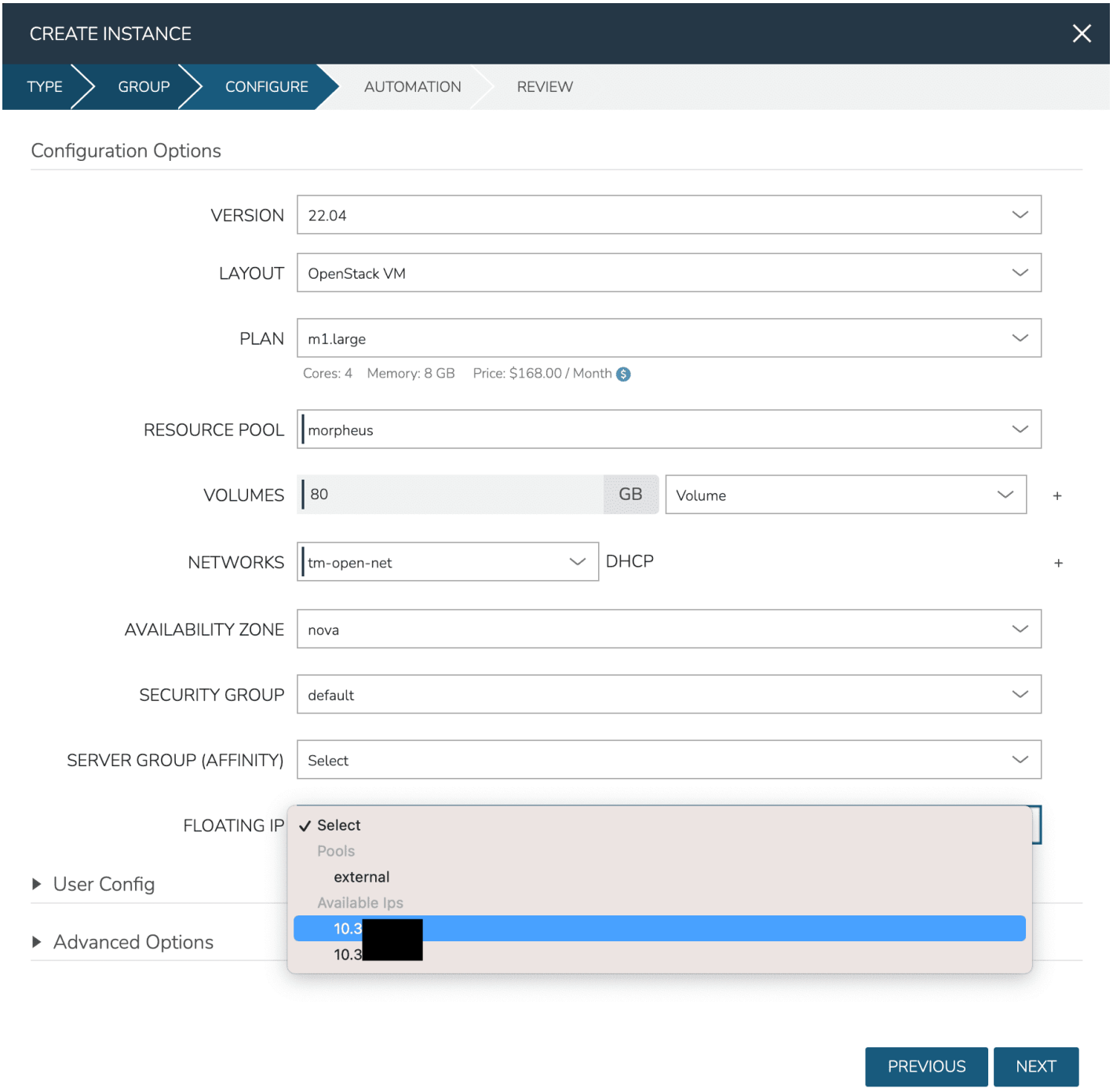
- **IP ADDRESS:** The address for the floating IP synced from a supported Cloud
- **CLOUD:** The Cloud integration the floating IP was synced from
- **STATUS:** "Free" when the floating IP is available and "Assigned" when the floating IP is currently assigned to a workload
- **VM:** For assigned floating IPs, the VM which currently has the floating IP attached

Free floating IPs will have a gear icon (⚙) at the end of the row. Click the gear icon and select "Release Floating IP" to release from within the source cloud and remove the entry from the Floating IPs list.

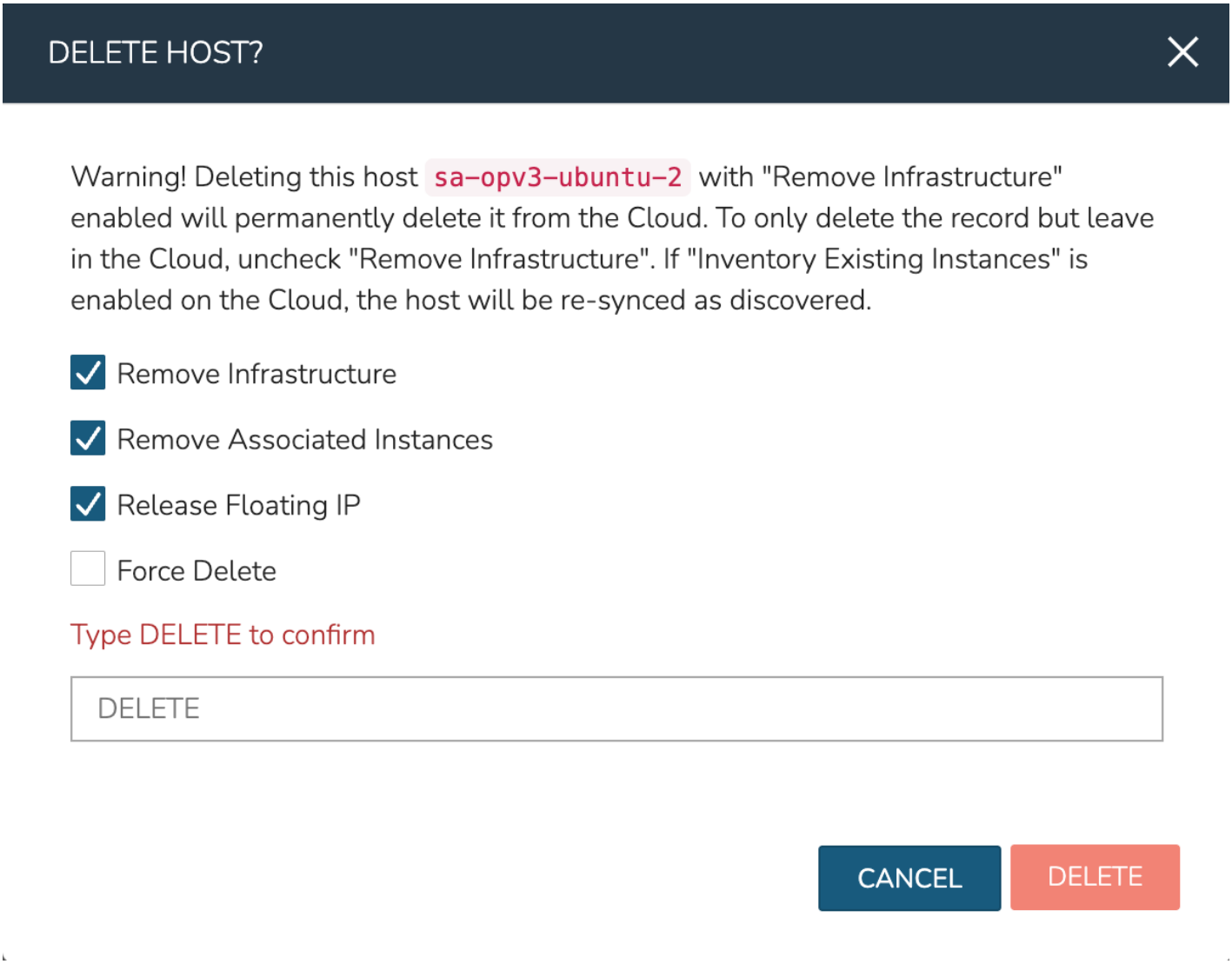


Working with Floating IPs

When provisioning to supported Clouds, VM Essentials will give the option to attach a floating IP at provision time. From the CONFIGURE tab of the provisioning wizard for supported Clouds, select the desired floating IP.



During Instance teardown, VM Essentials gives the option to release the floating IP.


DELETE HOST?
Warning! Deleting this host sa-opv3-ubuntu-2 with "Remove Infrastructure" enabled will permanently delete it from the Cloud. To only delete the record but leave in the Cloud, uncheck "Remove Infrastructure". If "Inventory Existing Instances" is enabled on the Cloud, the host will be re-synced as discovered.
Remove Infrastructure
Remove Associated Instances
Release Floating IP
Force Delete
Type DELETE to confirm
DELETE
CANCEL
DELETE

Domains

Infrastructure > Network > Domains

Subtopics

- Overview
- Adding Domains
- Editing Domain Permissions
- Editing and Removing Domains
- Setting the default domain on a Cloud
- Setting the default domain on a Network
- Selecting a Domain while provisioning an Instance

Overview

The Domains section is for creating and managing domains for use in VM Essentials. Domains are used for setting FQDNs, joining Domains, and creating DNS records. The Domains section is also a multi-tenant endpoint for managing domain settings across multiple tenants.

- Domains are synced in from Cloud, DNS and Network Integrations. Domains can also be user created.
- Active Domains are available for selection in the Domain dropdown when provisioning an Instance
- Default Domains can be set for Clouds and Networks in their Advanced Options sections.
- Images can be flagged to Auto-Join Domains in the Infrastructure > Network > Domains section

> **IMPORTANT**
> For an Instance to auto-join a Domain, a Domain must set in the Advanced Options section of the Cloud or Network used when provisioning

Adding Domains

Procedure

1. Navigate to Infrastructure > Network > Domains
2. Select + ADD
3. Enter the following:

Domain Name

Ex. demo.example.com

Description

Descriptive metadata for use in VM Essentials

Display Name

Overrides the displayed name in domain selection components, which is useful when using many OU paths

Public Zone

Check for Public Zones, leave uncheck for Private Zones

Workflow

Select an existing Workflow which will be applied to Instances at provision time when they are associated with the domain. This is useful for any domain-related scripting you may currently use. For example, you may want to ensure a machine is removed from the domain when it's torn down which could be accomplished by creating a Provisioning Workflow (with teardown phase Tasks) and associating the Workflow with the domain

Active

Active Domains are available for selection in Domain selection fields across VM Essentials. Inactive Domains are removed from Domain selection fields.

Join Domain Controller

Enable to have Windows instances join a Domain

Username

Admin user for Domain. `domain\username` format required when specifying OU Path

Password

Password for DC user account

DC Server

(optional) Specify the URL or Path of the DC Server

OU Path

(optional) Enter the OU Path for the connection string.

Guest Username

(optional) If set, this will change the provisioned hosts RPC Service User after domain join. Useful when a domain policy disables the Administrator account that typically would be set as the RPC user on a host record. VM Essentials will update the RPC username and password on the host(s) record after domain join with the specified Guest Username and Guest Password. The RPC username and password are used for auth during Remote Procedure Call (RPC) executions over winrm, ssh and guest tools.

Guest Password

(optional) The password for the Guest User account indicated in the prior field

4. Click Save Changes

Results

The Domain has been added and will be selectable in the Domain dropdown during provisioning, and in Cloud and Network settings.

Editing Domain Permissions

To edit visibility permissions for a domain, navigate to Infrastructure > Network > Domains. In the row for the selected domain, click MORE > Permissions. Within the Permissions modal, set Group access permissions.

Subtopics

Group Access

Group Access

The Group Access control affects which Groups have access to the domain at provision time. Select “all” to allow workloads provisioned to any Group access to the domain. If specific Groups are selected, only workloads provisioned to those Groups will have visibility of the domain during provisioning.

Editing and Removing Domains

- Domains can be edited by selecting the Actions dropdown for the Domain and selecting Edit, or by selecting the ✎ icon in list views.
- Added Domains can be removed from VM Essentials by selecting the Actions dropdown for the Domain and selecting Remove, or the icon in list views.

Setting the default domain on a Cloud

Procedure

1. Navigate to Infrastructure > Clouds.

2. Edit the target Cloud.
3. Expand Advanced Options section.
4. In the *Domain* dropdown, select the Domain.
5. Save Changes

Setting the default domain on a Network

Procedure

1. Navigate to Infrastructure > Network.
2. Edit the target Network.
3. Expand Advanced Options section.
4. In the *Domain* dropdown, select the Domain.
5. Save Changes

Selecting a Domain while provisioning an Instance

Procedure

1. While creating an instance, in the Configure section, expand the DNS Options.
2. Select Domain from the *Domain* dropdown.

Proxies

Subtopics

Overview
Defining Proxies
Cloud Communication
Provisioning with Proxies

Overview

In many situations, organizations deploy virtual machines in proxy restricted environments for things such as PCI Compliance, or just general security. As a result of this VM Essentials provides out of the box support for proxy connectivity. Proxy authentication support is also provided with both Basic Authentication capabilities as well as NTLM for Windows Proxy environments. VM Essentials is even able to configure virtual machines it provisions to utilize these proxies by setting up the operating systems proxy settings directly (restricted to cloud-init based Linux platforms for now, but can also be done on windows based platforms in a different manner).

To get started with Proxies, it may first be important to configure the VM Essentials appliance itself to have access to proxy communication for downloading service catalog images. To configure this, visit the Administration > Settings page where a section labeled “Proxy Settings” is located. Fill in the relevant connection info needed to utilize the proxy. It may also be advised to ensure that the Linux environment’s `http_proxy`, `https_proxy`, and no_proxy are set appropriately.

Defining Proxies

Proxies can be used in a few different contexts and optionally scoped to specific networks with which one may be provisioning into or on a cloud integration as a whole. To configure a Proxy for use by the provisioning engines within VM Essentials we must go to Infrastructure > Networks > Proxies. Here we can create records representing connection information for various proxies. This includes the host ip address, proxy port, and any credentials (if necessary) needed to utilize the proxy. Now that these proxies are defined we can use them in various contexts.

Cloud Communication

When morpheus needs to connect to various cloud APIs to issue provisioning commands or to sync in existing environments, we need to ensure that those api endpoints are accessible by the appliance. In some cases the appliance may be behind a proxy when it comes to public cloud access like Azure and AWS. To configure the cloud integration to utilize a proxy, when adding or editing a cloud there is a setting called “API Proxy” under “Advanced Options”. This is where the proxy of choice can be selected to instruct the Provisioning engine how to communicate with the public cloud. Simply adjust this setting and the cloud should start being able to receive/issue instructions.

Provisioning with Proxies

Proxy configurations can vary from operating system to operating system and in some cases it is necessary for these to be configured in the blueprint as a prerequisite. In other cases it can also be configured automatically. Mostly with the use of cloud-init (which all of our out of the box service catalog utilizes on all clouds). When editing/creating a cloud there is a setting for “Provisioning Proxy” in “Provisioning Options”. If this proxy is set, VM Essentials will automatically apply these proxy settings to the guest operating system.

Overriding proxy settings can also be done on the Network record. Networks (or subnets) can be configured in Infrastructure > Networks or on the Networks tab of the relevant Cloud detail page. Here, a proxy can also be assigned as well as additional options like the No Proxy rules for proxy exceptions.

Integrations

Subtopics

- Overview
- Scoping Services

Overview

The Network Integrations section allows you to add and manage IPAM, DNS, and Service Registry integrations.

Scoping Services

NETWORKING

Networking integrations are available in the NETWORK MODE dropdown located under the Advanced Options section in Cloud configurations.

IPAM

IPAM integrations will populate pools in the IP Pool section, which are available for assignment to networks in the NETWORK POOL dropdown when configuring a network.

SECURITY

Security integrations are available in the SECURITY SERVER dropdown located under the Advanced Options section in Cloud configurations.

DNS

DNS integrations will populate domains in the Infrastructure > Network > Domains section, and are available in the DOMAIN dropdown located under the Advanced Options section in Cloud, Group, and Network configurations, as well as in the Configure section of the Create Instance wizard. DNS integrations are also available in the DNS SERVICE dropdown located under the Advanced Options section in Cloud and Group configurations.

Service Registry

Service Registry integrations are available in the SERVICE REGISTRY dropdown located under the Advanced Options section in Cloud and Group configurations.

NOTE

Infoblox will also appear as a DNS INTEGRATION option in Clouds and Groups after adding Infoblox IPAM Integration.

Storage

Infrastructure > Storage is for adding and managing Storage Buckets, File Shares, Volumes, Data Stores and Storage Servers for use with other Services in VM Essentials.

Subtopics

- Role Requirements
- Default Storage
- Supported Bucket Types
- Alibaba Buckets
- Amazon S3 Buckets
- Azure Buckets
- Google Cloud Storage Buckets
- Dell EMC ECS Buckets
- Openstack Swift Buckets
- Rackspace CDN Buckets
- Supported File Share Types
- CIFS File Shares
- Local Storage File Shares
- NFSv3 File Shares
- Create Data Stores
- Manage Permissions
- Add Storage Server

Role Requirements

There are two Role permissions for the Infrastructure > Storage section: Infrastructure: Storage and Infrastructure: Storage Browser. Infrastructure: Storage gives Full, Read or No access to the Infrastructure > Storage sections, while Infrastructure: Storage Browser is specific to Buckets and Files Shares. Full Infrastructure: Storage Browser permissions allows Buckets and Files Shares to be browsed and files and folders to be added, downloaded and deleted from the Buckets and Files Shares. Read Infrastructure: Storage Browser permissions

allows Buckets and Files Shares to be browsed only.

Default Storage

The default Storage path for Virtual Images, Backups, Deployment Archives, Archive Service, and Archived Snapshots is `var/opt/morpheus/morpheus-ui/`. It is recommended to add Storage Buckets and File Shares for these targets in the Infrastructure > Storage section to avoid running out of disk space on the VM Essentials Appliance.

Subtopics

- Storage Buckets

Storage Buckets

Storage Buckets are for Backup, Archives, Deployment and Virtual Images storage targets. Buckets can be browsed and files and folders can be uploaded, downloaded or deleted from the Bucket section. Retention Policies can be set on Storage Buckets for files to be deleted or backed up to another bucket after a set amount of time.

Supported Bucket Types

- Alibaba
- Amazon S3
- Azure
- Google Cloud Storage
- Openstack Swift
- Rackspace CDN
- Generic S3

Alibaba Buckets

About this task

To Add an Alibaba Storage Bucket:

Procedure

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the BUCKETS tab, Click the + ADD button.
4. Select Alibaba from the dropdown list
5. From the NEW BUCKET Wizard input the following:

NAME

Name of the Bucket in VM Essentials.

ACCESS KEY

Alibaba Access Key

SECRET KEY

Alibaba Secret Key

REGION

Enter Alibaba Region for the Bucket

BUCKET NAME

Enter existing Alibaba Bucket name, or to add a new Bucket enter a new name and select Create Bucket.

Create Bucket

Enable if the Bucket entered in BUCKET NAME does not exist and needs to be created.

Default Backup Target

Sets this Bucket as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this Bucket will be presented.

Archive Snapshots

Enabled to export VM snapshots to this Bucket when creating VMware Backups, after which the snapshot will be removed from the target hypervisor.

Default Deployment Archive Target

Sets this bucket as the default storage target when uploading Deployment files in the Deployments section.

Default Virtual Image Store

Sets this bucket as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

RETENTION POLICY

None

Files in the Bucket will not be automatically deleted or backed up.

Backup Old Files

This option will backup files after a set amount of time and remove them from the bucket.

DAYS OLD

Files older than the set number of days will be automatically backed up to the selected Backup Bucket.

BACKUP BUCKET

Search for and then select the Bucket the files will be backed up to.

DELETE OLD FILES

This option will delete files from this bucket after a set amount of days.

DAYS OLD

Files older than the set number of days will be automatically deleted from the Bucket.

6. Select SAVE CHANGES

Results

The Bucket will be created and displayed in the Buckets tab.

- To browse, upload, download, or delete files from this Bucket, select the name of the Bucket.
- To edit the Bucket, select the edit icon or select the name of the Bucket and select ACTIONS - EDIT.

> **WARNING**
>
> Repointing a bucket that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a Bucket, select the trash icon or select the name of the Bucket and select DELETE.

> **WARNING**
>
> When deleting a Bucket, all Deployment Versions and Backups associated with the Bucket will be deleted.

Amazon S3 Buckets

About this task

To Add an Amazon S3 Storage Bucket:

Procedure

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the BUCKETS tab, Click the + ADD button.
4. Select Amazon S3 from the dropdown list
5. From the NEW BUCKET Wizard input the following:

   NAME

   Name of the Bucket in VM Essentials.

   ACCESS KEY

   AWS IAM Access Key

   SECRET KEY

   AWS IAM Secret Key

   BUCKET NAME

   Enter existing S3 Bucket name, or to add a new Bucket enter a new name and select Create Bucket.

   CREATE BUCKET

   Enable if the Bucket entered in BUCKET NAME does not exist and needs to be created. If enabled, select an AWS Region to create the Bucket in.

   ENDPOINT URL

   Optional endpoint URL if pointing to an object store other than amazon that mimics the Amazon S3 APIs.

   Default Backup Target

Sets this Bucket as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this Bucket will be presented.

Archive Snapshots

Enabled to export VM snapshots to this Bucket when creating VMware Backups, after which the snapshot will be removed from the target hypervisor.

Default Deployment Archive Target

Sets this bucket as the default storage target when uploading Deployment files in the Deployments section.

Default Virtual Image Store

Sets this bucket as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

RETENTION POLICY

None

Files in the Bucket will not be automatically deleted or backed up.

Backup Old Files

This option will backup files after a set amount of time and remove them from the bucket.

DAYS OLD

Files older than the set number of days will be automatically backed up to the selected Backup Bucket.

BACKUP BUCKET

Search for and then select the Bucket the files will be backed up to.

DELETE OLD FILES

This option will delete files from this bucket after a set amount of days.

DAYS OLD

Files older than the set number of days will be automatically deleted from the Bucket.

6. Select SAVE CHANGES

Results

The Bucket will be created and displayed in the Buckets tab.

- To browse, upload, download, or delete files from this Bucket, select the name of the Bucket.
- To edit the Bucket, select the edit icon or select the name of the Bucket and select ACTIONS - EDIT.

WARNING

Repointing a bucket that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a Bucket, select the trash icon or select the name of the Bucket and select DELETE.

WARNING

When deleting a Bucket, all Deployment Versions and Backups associated with the Bucket will be deleted.

Azure Buckets

About this task

To Add an Azure Storage Bucket:

Procedure

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the BUCKETS tab, Click the + ADD button.
4. Select Azure from the dropdown list
5. From the NEW BUCKET Wizard input the following:

NAME

Name of the Bucket in VM Essentials.

STORAGE ACCOUNT

Name of the Storage Account in Azure for the Bucket

STORAGE KEY

Storage Key provided from Azure

SHARE NAME

Enter existing Azure Storage Share name, or to add a new Share enter a new name and select Create Bucket below.

CREATE BUCKET

Enable if the Share entered in SHARE NAME does not exist and needs to be created.

Default Backup Target

Sets this bucket as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this Bucket will be presented.

Archive Snapshots

Enabled to export VM snapshots to this Bucket when creating VMware Backups, after which the snapshot will be removed from the target hypervisor.

Default Deployment Archive Target

Sets this Bucket as the default storage target when uploading Deployment files in the Deployments section.

Default Virtual Image Store

Sets this bucket as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

RETENTION POLICY

None

Files in the Bucket will not be automatically deleted or backed up.

Backup Old Files

This option will backup files after a set amount of time and remove them from the bucket.

DAYS OLD

Files older than the set number of days will be automatically backed up to the selected Backup Bucket.

BACKUP BUCKET

Search for and then select the Bucket the files will be backed up to.

DELETE OLD FILES

This option will delete files from this bucket after a set amount of days.

DAYS OLD

Files older than the set number of days will be automatically deleted from the Bucket.

6. Select SAVE CHANGES

Results

The Bucket will be created and displayed in the Buckets tab.

- To browse, upload, download, or delete files from this Bucket, select the name of the Bucket.
- To edit the Bucket, select the edit icon or select the name of the Bucket and select ACTIONS - EDIT.

> **WARNING**
>
> **Repointing a bucket that is in use may cause loss of file references. Ensure data is mirrored first.**

- To delete a Bucket, select the trash icon or select the name of the Bucket and select DELETE.

> **WARNING**
>
> **When deleting a Bucket, all Deployment Versions and Backups associated with the Bucket will be deleted.**

Google Cloud Storage Buckets

About this task

> **NOTE**
>
> Google Cloud Storage Buckets are associated with an existing GCP Cloud integration. Ensure the GCP Cloud integration is pre-existing before attempting to create a new Google Cloud Storage Bucket. On the initial integration and subsequent cloud syncs, Google Cloud Storage Buckets are automatically onboarded and updated.

To add a Google Cloud Storage Bucket:

Procedure

1. Select the Infrastructure link in the navigation bar
2. Select the Storage link in the sub-navigation bar
3. In the BUCKETS tab, Click the + ADD button
4. Select Google Cloud Storage from the dropdown list
5. From the NEW BUCKET Wizard input the following:

   NAME

A friendly name for the bucket in VM Essentials

STORAGE SERVICE

Select the GCP cloud integration this bucket should be created in

PROJECT ID

Select the Project to create the group under, Projects are a GCP-specific concept and are logical grouping for your resources. Select any existing project associated with your selected GCP cloud integration

BUCKET NAME

The name for the bucket resource on the GCP side

LOCATION TYPE

Select Region, Dual-Region, or Multi-Region. Buckets with a Region location type will be stored in one GCP region, such as “us-east1 (South Carolina)”. Dual-Region and Multi-Region data is stored in two (or more, in the case of multi-region) GCP regions separated by a significant physical distance. Dual-Region and Multi-Region data is geo-redundant across the multiple selected regions

LOCATION

A selected GCP region (or regions, in the case of dual and multi-location data) where the data will be stored

STORAGE CLASS

Select Standard, Nearline, Coldline, or Archive. The appropriate storage class will depend on how frequently the bucket data is accessed and how long the type of data in the bucket is expected to be stored. More information on storage classes can be found in **GCP Documentation**

ACTIVE

When marked, the bucket is available for use in VM Essentials

DEFAULT BACKUP TARGET

Sets the bucket as the default storage option when creating backups at provision time or in the Backups section of VM Essentials

DEFAULT DEPLOYMENT ARCHIVE TARGET

Sets this Bucket as the default storage target when uploading deployment files in the Deployments section

DEFAULT VIRTUAL IMAGE STORE

Sets this bucket as the default storage target when uploading virtual images from the Virtual Images section, importing images from Instance actions, creating images with the Image Builder, and when creating new images from Migrations

RETENTION POLICY

Select None and the files in this bucket will never be deleted or backed up by VM Essentials. When selecting ‘Backup Old Files’, VM Essentials will backup files into another selected bucket once they reach a certain number of days old. When selecting ‘Delete Old Files’, VM Essentials will delete any files that reach a certain number of days old

Dell EMC ECS Buckets

About this task

NOTE

A Dell EMC ECS Storage Server must be configured in Infrastructure - Storage - Servers prior to adding a Dell EMC ECS Bucket.

To Add a Dell EMC ECS Storage Bucket:

Procedure

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the BUCKETS tab, Click the + ADD button.
4. Select Dell EMC ECS Bucket from the dropdown list
5. From the NEW BUCKET Wizard input the following:

NAME

Name of the Bucket in VM Essentials.

STORAGE SERVICE

Select existing Dell EMC ECS Storage Server (configured in Infrastructure - Storage - Servers)

BUCKET NAME

Enter a name for the new Dell EMC ECS bucket.

USER

Dell EMC ECS User

SECRET KEY

Dell EMC ECS Secret key

NAMESPACE

Select Dell EMC ECS Namespace for the Bucket

STORAGE GROUP

Select a Dell EMC ECS Storage Group

Default Backup Target

Sets this bucket as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this Bucket will be presented.

Archive Snapshots

Enabled to export VM snapshots to this Bucket when creating VMware Backups, after which the snapshot will be removed from the target hypervisor.

Default Deployment Archive Target

Sets this Bucket as the default storage target when uploading Deployment files in the Deployments section.

Default Virtual Image Store

Sets this bucket as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

RETENTION POLICY

None

Files in the Bucket will not be automatically deleted or backed up.

Backup Old Files

This option will backup files after a set amount of time and remove them from the bucket.

DAYS OLD

Files older than the set number of days will be automatically backed up to the selected Backup Bucket.

BACKUP BUCKET

Search for and then select the Bucket the files will be backed up to.

DELETE OLD FILES

This option will delete files from this bucket after a set amount of days.

DAYS OLD

Files older than the set number of days will be automatically deleted from the Bucket.

6. Select SAVE CHANGES

Results

The Bucket will be created and displayed in the Buckets tab.

- To browse, upload, download, or delete files from this Bucket, select the name of the Bucket.
- To edit the Bucket, select the edit icon or select the name of the Bucket and select ACTIONS - EDIT.

> **WARNING**
>
> Repointing a bucket that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a Bucket, select the trash icon or select the name of the Bucket and select DELETE.

> **WARNING**
>
> When deleting a Bucket, all Deployment Versions and Backups associated with the Bucket will be deleted.

Openstack Swift Buckets

About this task

To Add an OpenStack Swift Bucket:

Procedure

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the BUCKETS tab, Click the + ADD button.
4. Select Openstack Swift from the dropdown list
5. From the NEW BUCKET Wizard input the following:

NAME

Name of the Bucket in VM Essentials.

USERNAME

Openstack Swift Username

API KEY

Openstack Swift API Key

BUCKET NAME

Enter existing Openstack Swift Bucket name, or to add a new Bucket enter a new name and select Create Bucket below.

IDENTITY URL

Openstack Swift Identity URL

Create Bucket

Enable if the name entered in BUCKET NAME does not exist and needs to be created.

Default Backup Target

Sets this bucket as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this Bucket will be presented.

Archive Snapshots

Enabled to export VM snapshots to this Bucket when creating VMware Backups, after which the snapshot will be removed from the target hypervisor.

Default Deployment Archive Target

Sets this Bucket as the default storage target when uploading Deployment files in the Deployments section.

Default Virtual Image Store

Sets this bucket as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

RETENTION POLICY

None

Files in the Bucket will not be automatically deleted or backed up.

Backup Old Files

This option will backup files after a set amount of time and remove them from the bucket.

DAYS OLD

Files older than the set number of days will be automatically backed up to the selected Backup Bucket.

BACKUP BUCKET

Search for and then select the Bucket the files will be backed up to.

DELETE OLD FILES

This option will delete files from this bucket after a set amount of days.

DAYS OLD

Files older than the set number of days will be automatically deleted from the Bucket.

6. Select SAVE CHANGES

Results

The Bucket will be created and displayed in the Buckets tab.

- To browse, upload, download, or delete files from this Bucket, select the name of the Bucket.
- To edit the Bucket, select the edit icon or select the name of the Bucket and select ACTIONS - EDIT.

WARNING

Repointing a bucket that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a Bucket, select the trash icon or select the name of the Bucket and select DELETE.

WARNING

When deleting a Bucket, all Deployment Versions and Backups associated with the Bucket will be deleted.

Rackspace CDN Buckets

About this task

To Add a Rackspace CDN Bucket:

Procedure

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the BUCKETS tab, Click the + ADD button.
4. Select Rackspace CDN from the dropdown list
5. From the NEW BUCKET Wizard input the following:

NAME

Name of the Bucket in VM Essentials.

USERNAME

Rackspace CDN Username

API KEY

Rackspace CDN API Key

REGION

Enter Rackspace CDN Region

BUCKET NAME

Enter existing Rackspace CDN Bucket name, or to add a new Bucket enter a new name and select Create Bucket below.

Create Bucket

Enable if the name entered in BUCKET NAME does not exist and needs to be created.

Default Backup Target

Sets this bucket as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this Bucket will be presented.

Archive Snapshots

Enabled to export VM snapshots to this Bucket when creating VMware Backups, after which the snapshot will be removed from the target hypervisor.

Default Deployment Archive Target

Sets this Bucket as the default storage target when uploading Deployment files in the Deployments section.

Default Virtual Image Store

Sets this bucket as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

RETENTION POLICY

None

Files in the Bucket will not be automatically deleted or backed up.

Backup Old Files

This option will backup files after a set amount of time and remove them from the bucket.

DAYS OLD

Files older than the set number of days will be automatically backed up to the selected Backup Bucket.

BACKUP BUCKET

Search for and then select the Bucket the files will be backed up to.

DELETE OLD FILES

This option will delete files from this bucket after a set amount of days.

DAYS OLD

Files older than the set number of days will be automatically deleted from the Bucket.

6. Select SAVE CHANGES

Results

The Bucket will be created and displayed in the Buckets tab.

- To browse, upload, download, or delete files from this Bucket, select the name of the Bucket.
- To edit the Bucket, select the edit icon or select the name of the Bucket and select ACTIONS - EDIT.

> **WARNING**
>
> Repointing a bucket that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a Bucket, select the trash icon or select the name of the Bucket and select DELETE.

> **WARNING**
>
> When deleting a Bucket, all Deployment Versions and Backups associated with the Bucket will be deleted.

Subtopics

File Shares

File Shares

File Shares are for Backup, Archives, and Virtual Images storage targets. File Shares can be browsed and files and folders can be uploaded,

downloaded or deleted from the File Shares section. Retention Policies can be set on Storage File Shares for files to be deleted or backed up to another File Share after a set amount of time.

Supported File Share Types

- CIFS (Samba Windows File Sharing)
- Local Storage
- NFSv3

CIFS File Shares

About this task

To Add a CIFS File Share:

Procedure

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the FILE SHARES tab, Click the + ADD button.
4. Select CIFS (Samba Windows File Sharing) from the dropdown list
5. From the NEW FILE SHARE Wizard input the following:

   NAME

   Name of the File Share in VM Essentials.

   HOST

   Enter host IP or resolvable hostname

   Example: `192.168.200.210`

   USERNAME

   CIFS Share Username

   PASSWORD

   CIFS Share User Password

   SHARE PATH

   Enter CIFS Share Path

   Example: `cifs`

   Default Backup Target

   Sets this File Share as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this File Share will be presented.

   Archive Snapshots

   Enabled to export VM snapshots to this File Share when creating VMware Backups, after which the snapshot will be removed from

the source Cloud.

Default Deployment Archive Target

Sets this File Share as the default storage target when uploading Deployment files in the Deployments section.

Default Virtual Image Store

Sets this File Share as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

RETENTION POLICY

None

Files in the File Share will not be automatically deleted or backed up.

Backup Old Files

This option will backup files after a set amount if time and remove them from the File Share.

DAYS OLD

Files older than the set number of days will be automatically backed up to the selected Backup File Share.

BACKUP File Share

Search for and select the File Share the files will be backed up to.

DELETE OLD FILES

This option will delete files from this File Share after a set amount of days.

DAYS OLD

Files older than the set number of days will be automatically deleted from the File Share.

6. Select SAVE CHANGES

Results

The File Share will be created and displayed in the File Shares tab.

- To browse, upload, download, or delete files from this File Share, select the name of the File Share.
- To edit the File Share, select the edit icon or select the name of the File Share and select ACTIONS - EDIT.

> **WARNING**
> Repointing a File Share that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a File Share, select the trash icon or select the name of the File Share and select DELETE.

> **WARNING**
> When deleting a File Share, all Deployment Versions and Backups associated with the File Share will be deleted.

Local Storage File Shares

About this task

IMPORTANT

Local Storage refers to local to the VM Essentials Appliance and the path must be owned by morpheus-app. Please be conscious of storage space. High Availability configurations require Local Storage File Shares paths to be shared storage paths between the font end VM Essentials Appliances.

NOTE

To change the owner of a file path to be used as a Local Storage File Share, run `chown morpheus-app:morpheus-app /path` on the VM Essentials Appliance.

NOTE

VM Essentials will validate path and ownership of the File Share Path.

To Add a Local Storage File Share:

Procedure

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the FILE SHARES tab, Click the + ADD button.
4. Select Local Storage Share from the dropdown list
5. From the NEW FILE SHARE Wizard input the following:

NAME

Name of the File Share in VM Essentials.

STORAGE PATH

Enter the File Share path on the local VM Essentials Appliance.

Example: `/var/opt/morpheus/morpheus-ui/vms/virtual-images`

IMPORTANT

High Availability configurations require Local Storage File Shares paths to be shared storage paths between the font end VM Essentials Appliances.

Default Backup Target

Sets this File Share as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this File Share will be presented.

Archive Snapshots

Enabled to export VM snapshots to this File Share when creating VMware Backups, after which the snapshot will be removed from the source Cloud.

Default Deployment Archive Target

Sets this File Share as the default storage target when uploading Deployment files in the Deployments section.

Default Virtual Image Store

Sets this File Share as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

RETENTION POLICY

None

Files in the File Share will not be automatically deleted or backed up.

Backup Old Files

This option will backup files after a set amount if time and remove them from the File Share.

DAYS OLD

Files older than the set number of days will be automatically backed up to the selected Backup File Share.

BACKUP File Share

Search for and select the File Share the files will be backed up to.

DELETE OLD FILES

This option will delete files from this File Share after a set amount of days.

DAYS OLD

Files older than the set number of days will be automatically deleted from the File Share.

6. Select SAVE CHANGES

Results

The File Share will be created and displayed in the File Shares tab.

- To browse, upload, download, or delete files from this File Share, select the name of the File Share.
- To edit the File Share, select the edit icon or select the name of the File Share and select ACTIONS - EDIT.

> **WARNING**
> **Repointing a File Share that is in use may cause loss of file references. Ensure data is mirrored first.**

- To delete a File Share, select the trash icon or select the name of the File Share and select DELETE.

> **WARNING**
> **When deleting a File Share, all Deployment Versions and Backups associated with the File Share will be deleted.**

NFSv3 File Shares

About this task

> **NOTE**
> Configure access to the NFS folder on the NFS Provider prior to adding the NFSv3 File Share.

> **NOTE**
> Upon save VM Essentials will create a persistent mount owned by `morpheus-app.morpheus-app` on the VM Essentials Appliance for the NFSv3 File Share. The VM Essentials appliance will require access to the following ports in order to mount the share: 111, 54302, 20048, 2049, 46666, 42955, 875. With some storage solutions, you may need to enable insecure, unprivileged ports, or allow non-root on the export before VM Essentials is able to successfully mount the share.

To Add a NFSv3 File Share:

Procedure

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the FILE SHARES tab, Click the + ADD button.
4. Select NFSv3 from the dropdown list
5. From the NEW FILE SHARE Wizard input the following:

   NAME

   Name of the File Share in VM Essentials.

   HOST

   Enter the File Share path on the local VM Essentials Appliance.

   EXPORT FOLDER

   Enter the NFSv3 Folder

   Default Backup Target

   Sets this File Share as the default backup target when creating Backups. If selected the option to update existing Backup configuration to use this File Share will be presented.

   Archive Snapshots

   Enabled to export VM snapshots to this File Share when creating VMware Backups, after which the snapshot will be removed from the source Cloud.

   Default Deployment Archive Target

   Sets this File Share as the default storage target when uploading Deployment files in the Deployments section.

   Default Virtual Image Store

   Sets this File Share as the default storage target when uploading Virtual Images from the Virtual Images section, importing Images from Instance Actions, creating Images with the Image Builder and when creating new images from Migrations.

   RETENTION POLICY

   None

   Files in the File Share will not be automatically deleted or backed up.

   Backup Old Files

   This option will backup files after a set amount if time and remove them from the File Share.

   DAYS OLD

   Files older than the set number of days will be automatically backed up to the selected Backup File Share.

   BACKUP File Share

   Search for and select the File Share the files will be backed up to.

   DELETE OLD FILES

   This option will delete files from this File Share after a set amount of days.

   DAYS OLD

   Files older than the set number of days will be automatically deleted from the File Share.

6. Select SAVE CHANGES

Results

The File Share will be created and displayed in the File Shares tab.

- To browse, upload, download, or delete files from this File Share, select the name of the File Share.
- To edit the File Share, select the edit icon or select the name of the File Share and select ACTIONS - EDIT.

> **WARNING**
>
> Repointing a File Share that is in use may cause loss of file references. Ensure data is mirrored first.

- To delete a File Share, select the trash icon or select the name of the File Share and select DELETE.

> **WARNING**
>
> When deleting a File Share, all Deployment Versions and Backups associated with the File Share will be deleted.

Subtopics

Data Stores

Data Stores

Data Stores are logical divisions of underlying storage disk. Organizations may use them to divide and track cloud resources by team or department. When integrating certain Cloud types, VM Essentials will onboard all existing data stores and administrators can then make them available to Groups as needed. At provision time, when applicable based on Cloud and Layout, users can select the datastore they wish to provision to.

Here within the Data Store view in the storage section, users can see a list of data stores for each Cloud. In the row for each Cloud, the storage type, associated Cloud, and permissions information are shown.

Create Data Stores

To a limited extent, data stores can be created from this view. In order to create a data store, you would need to first have an integrated 3Par server. See the section on storage servers for more information on setting up this integration.

> **NOTE**
>
> For all other data store types, create the needed data store within the target Cloud and VM Essentials will automatically sync in the data store on the next Cloud sync. You can force a Cloud sync from the Cloud Detail Page (Infrastructure > Clouds > Selected Cloud > RefreshMenu > Short).

- Navigate to Infrastructure > Storage > Data Stores
- Click +ADD
- Enter a Name, select a VMware Cloud, select a 3Par Volume, and select a Host Group
- Manage permissions in the Group Access and Tenant Permissions sections, if needed
- Click SAVE CHANGES

Manage Permissions

Manage Permissions

From this view, users can manage permissions for any data store synced from integrated Clouds. This includes setting which Groups have access to the data store. To edit data store permissions:

- Navigate to Infrastructure > Storage > Data Stores
- Click ACTIONS > Edit
- **Groups:** Select “all” Groups or select specific Groups which should have access to the data store
- **Active:** When marked, the data store is active and available for provisioning
- Click SAVE CHANGES

Subtopics

Servers

Servers

Add Storage Server

Procedure

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the SERVERS tab, Click the + ADD button.
4. From the ADD STORAGE SERVER wizard input the following:

   NAME

   Name of the Storage Server in VM Essentials

   TYPE

   Select 3Par

   URL

   URL Of 3Par Server Example : `https://192.168.190.201:8008`

   USERNAME

   Add your administrative user account.

   PASSWORD

   Add your administrative password.
5. Select SAVE CHANGES

Results

The 3Par Storage Server will be added and displayed in the Buckets tab. Buckets, Files Shares and Storage Groups will be synced in.

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.

3. In the SERVERS tab, Click the + ADD button.
4. From the ADD STORAGE SERVER wizard input the following:

   NAME

   Name of the Storage Server in VM Essentials

   TYPE

   Select Dell EMC ECS

   URL

   URL Of DELL EMC ECS Server

   Example : `https://192.168.190.200:4443`

   TIP

   The port 4443 is the api port for ECS api. This may be different depending on your configuration

   USERNAME

   Add your administrative user account.

   PASSWORD

   Add your administrative password.

   S3 SERVICE URL (Optional)

   Add your S3 service url Example: **http://192.168.190.220:9020**

   NOTE

   S3 SERVICE URL is not required if you are not planning on using ECS S3.

5. Select SAVE CHANGES

The Dell EMC ECS Storage Server will be added and displayed in the Buckets tab. Buckets, Files Shares and Storage Groups will be synced in.

1. Select the Infrastructure link in the navigation bar.
2. Select the Storage link in the sub navigation bar.
3. In the SERVERS tab, Click the + ADD button.
4. From the ADD STORAGE SERVER wizard input the following:

   NAME

   Name of the Storage Server in VM Essentials

   TYPE

   Select Dell EMC Isilon

   URL

   URL Of Dell EMC Isilon Server Example : `https://192.168.190.202:8080`

   USERNAME

   Add your administrative user account.

   PASSWORD

   Add your administrative password.

PROVISION USER

Select Provision User

PROVISION GROUP

Select Provision Group

ROOT PATH

Enter Root Path

Example : `\`

5. Select SAVE CHANGES

The Dell EMC Isilon Storage Server will be added and displayed in the Buckets tab. Buckets, Files Shares and Storage Groups will be synced in.

Trust

The Trust section is where credentials and SSH keypairs are stored. Stored credentials are useful for easy integration with VMware Clouds or other third party technologies using stored credential sets. In the keypairs section, generate SSH keypairs which can be associated with your user account so that your public key is automatically added to the authorized keys file on provisioned workloads for easy access.

Subtopics

Credentials
OAuth 2.0 Credentials
Key Pairs

Credentials

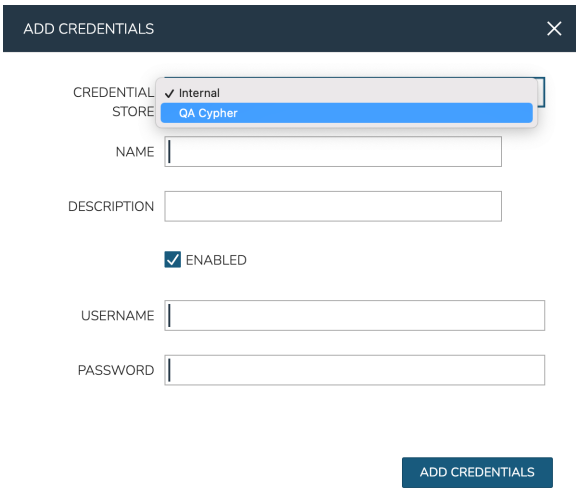
The credentials section allows for various credential types to be securely stored and called back when necessary, such as when creating new integrations with Cloud accounts or other outside technologies. Credentials can also be used to populate REST-based Option Lists sourced from data behind an authentication wall, as well as to run automation Tasks on remote targets that require authentication. Credentials are stored internally and securely on the VM Essentials appliance. The following credential pair types are currently supported:

- Access Key and Secret Key
- Client ID and Secret
- Email and Private Key
- OAuth 2.0
- Tenant, Username, and Keypair
- Username and API Key
- Username and Keypair
- Username and Password
- Username, Password, and Keypair

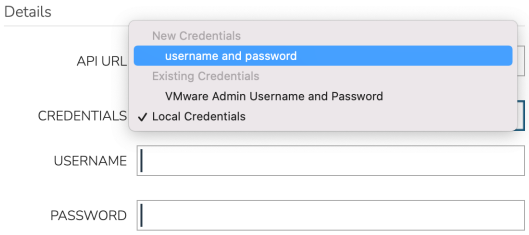
To create a new credential set, click + ADD and then select the type of credential set you'd like to store. Complete the following:

- **CREDENTIAL STORE:** Select "Internal", an integrated external Cypher store (if any), or an integrated Hashicorp Vault server (if any). See the section below for instructions on integrating with Vault or standing up and integrating with an external Cypher store.
- **NAME:** A name for the credential set in VM Essentials

- **DESCRIPTION:** An optional description for the credential set
- **ENABLED:** If checked, the credential set will be available for use
- **CREDENTIAL VALUES:** Depending on the credential pair type selected (listed above), the remaining fields will be specific to the chosen type. See the next section for a more complete walkthrough on storing and using OAuth 2.0 credentials



Finally, click ADD CREDENTIALS. Once saved, the credential set will be available for selection where appropriate in VM Essentials UI. In the screenshot below, I'm integrating a new VMware Cloud. In the credentials section, I have the following options: Creating (and using) a new Username and Password credential set (which includes the option to save internally or to an external Cypher store), choosing a previously-stored credential set, or simply entering my credentials locally and not saving them for reuse.



OAuth 2.0 Credentials

VM Essentials supports storage of credential sets for retrieving temporary access tokens, through OAuth 2.0, and using the tokens to access some resource. These credential sets can be used with REST-type Option Lists to retrieve information behind this type of authentication wall. Once stored, the credential can be used with as many Option Lists as needed and potentially in other areas of the product in the future.

To create a new credential set, click + ADD and then select "OAuth 2.0". Complete the following, not all fields are present or required in every context:

- **CREDENTIAL STORE:** Select "Internal" or an integrated external Cypher store (if any). See the next section for instructions on standing up and integrating with an external Cypher store
- **NAME:** A name for the credential set in VM Essentials
- **DESCRIPTION:** An optional description for the credential set
- **ENABLED:** If checked, the credential set will be available for use
- **GRANT TYPE:** Client Credentials or Password Credentials
- **ACCESS TOKEN URL:** The authorization server's token endpoint
- **CLIENT ID:** The client ID for an app registered with the target service
- **CLIENT SECRET:** The client secret, often needed when requesting access outside the context of a specific user

- **USERNAME:** (Only present with “Password Credentials” Grant Type) The username for a user with target data access
- **PASSWORD:** (Only present with “Password Credentials” Grant Type) The password for the user indicated above
- **SCOPE:** The scope of access requested to the target resource
- **CLIENT AUTHENTICATION:** “Send as basic auth header” or “Send client credentials in body” - Indicates how VM Essentials should issue the token received in requests to the target resource

Once done, click ADD CREDENTIALS.

Subtopics

Add Existing Key Pair
Generate Key Pair
Delete Key Pair

Add Existing Key Pair

About this task

To generate a existing Key Pair:

Procedure

1. Navigate to Infrastructure > Trust > Key Pairs
2. On the Key Pairs tab, click + ADD and select “Existing Key Pair”
3. From the Add Key Pair modal input the following as needed:
   - Name
   - Public Key
   - Private Key
   - Passphrase

NOTE

Certain features do not require storage of the private key.

Generate Key Pair

About this task

To generate a Key Pair:

Procedure

1. Navigate to Infrastructure > Trust > Key Pairs
2. On the Key Pairs tab, click + ADD and select “Existing Key Pair”
3. After naming the new key pair, VM Essentials will reveal both the public and private key

Results

NOTE

After the private key is initially revealed it will not be shown again. If needed, you may view the public key from the Keypairs list page at any time going forward. This key pair can be associated with your Linux user details in VM Essentials user settings. The public key will be added to the authorized_keys file on provisioned workloads where your Linux user is added at provision time.

Delete Key Pair

About this task

To Delete Key Pair:

Procedure

1. Navigate to Infrastructure > Trust > Key Pairs
2. On the Key Pairs tab, select the trash can icon at the end of any row
3. Acknowledge that you wish to delete the selected key pair

Key Pairs

The key pairs section enables the following actions: Add and Delete key pairs. Key pairs are commonly used by HPE Morpheus VM Essentials for accessing instances via SSH. HPE Morpheus VM Essentials stores key pairs to simplify administration and access across both private and public clouds.

HPE Morpheus VM Essentials only accepts key pairs in PEM format (for example, a private key beginning with `-----BEGIN RSA PRIVATE KEY-----`) and accepts RSA (PKCS#1 or PKCS#8, default), DSA (PKCS#1 or PKCS#8), EC (PKCS#8), and ed25519 (PKCS#8) keys. If you have a key in another format, such as OpenSSH, convert the key:

```
#No passphrase
ssh-keygen -m pem -f /path/to/key
#With passphrase
ssh-keygen -p -P "old passphrase" -N "new passphrase" -m pem -f path/to/key
```

Subtopics

Add Existing Key Pair
Generate Key Pair
Delete Key Pair

Add Existing Key Pair

About this task

To generate a existing Key Pair:

Procedure

1. Navigate to Infrastructure > Trust > Key Pairs
2. On the Key Pairs tab, click + ADD and select “Existing Key Pair”

3. From the Add Key Pair modal input the following as needed:
    - Name
    - Public Key
    - Private Key
    - Passphrase

> **NOTE**
> Certain features do not require storage of the private key.

Generate Key Pair

About this task

To generate a Key Pair:

Procedure

1. Navigate to Infrastructure > Trust > Key Pairs
2. On the Key Pairs tab, click + ADD and select “Generate Key Pair”
3. After naming the new key pair, HPE Morpheus VM Essentials will reveal both the public and private key

Results

> **NOTE**
> After the private key is initially revealed it will not be shown again. If needed, you may view the public key from the Keypairs list page at any time going forward. This key pair can be associated with your Linux user details in HPE Morpheus VM Essentials user settings. The public key will be added to the authorized_keys file on provisioned workloads where your Linux user is added at provision time.

Delete Key Pair

About this task

To Delete Key Pair:

Procedure

1. Navigate to Infrastructure > Trust > Key Pairs
2. On the Key Pairs tab, select the trash can icon at the end of any row
3. Acknowledge that you wish to delete the selected key pair

Backups

The VM Essentials built-in Backup solution provides VM, Container, Host, Database, File, Directory, Volume and Storage Provider Backup, Snapshot and Replication capabilities. Backups can be automatically configured during provisioning or manually created at any time. Backup Jobs with custom Execution Schedules and retention counts can be created and used across all environments in conjunction with configured Storage Providers. Backups can be restored over current Instances or as new Instances, and downloaded or deleted from VM Essentials.

VM Essentials also integrates with external services to automate availability with other providers.

Subtopics

- Initial Backups Setup
- Configuring Backups during Provisioning
- Summary
- Backups

Initial Backups Setup

Global Backup settings (Administration > Settings > Backups), Storage Providers (Infrastructure > Storage) and Execution Schedules (Library > Automation > Execute Scheduling) should be configured prior to creating backups. Global backup settings are where scheduled backups can be globally enabled or disabled and certain global backup default settings can be configured. Storage providers include local and remote configured storage locations that can be used as backup targets. Execution schedules are timed intervals at which individual automated backup jobs will run. See the next two sections for full details on global backup settings and configuring execution schedules. See VM Essentials UI **storage documentation** for more information about configuring local and remote storage targets and/or integrating with third party storage providers.

Subtopics

- Global Backups Settings
- Execution Schedules

Global Backups Settings

VM Essentials Backups can be enabled under Administration > Settings > Backups.

Scheduled Backups

When enabled, configured Backups will automatically run on their configured schedules. If disabled, backups need to be manually run.

Create Backups

When enabled, VM Essentials will automatically configure backup jobs for Instances at provision time.

Backup Appliance

When enabled, a Backup will be created to backup the VM Essentials appliance database. Select the `Backup` text link to edit the Appliance Backup Settings and view existing Appliance Backups.

Default Backup Bucket

From this dropdown, select the default storage bucket to be used for future created Backups. If needed, new storage providers can be configured and managed in the Infrastructure > Storage section.

Default Backup Schedule

From this dropdown, select a default execution schedule for future created Backups. If needed, new schedules can be configured in Library > Automation > Execute Scheduling.

Backup Retention Count

The default maximum number of successful backups to retain.

Default Synthetic Full Backup Enabled

When enabled, supported workload types will have periodic full synthetic backups scheduled by default in addition to any typical backups (full backup followed by incremental backups) that may also be scheduled.

Default Synthetic Full Backups Schedule

From this dropdown, select a default execution schedule for future full synthetic backups. In general, this should be at a longer internal than incremental backups that are also scheduled. If needed, new schedules can be configured in Library > Automation > Execute Scheduling.

Execution Schedules

Backup Execution Schedules can be configured and managed in Library > Automation > Execute Scheduling. An execution schedule stores only the interval at which some execution should be run and they can apply to both backups and automation scripts. To create a new backup job with this schedule, navigate to Backups > Backups and click "+ADD". In the final step of creating the backup job we are able to select any of our created execution schedules. The Default Backup Schedule set in Administration > Settings > Backups will be selected when creating a backup job and not specifying an execution schedule.

Configuring Backups during Provisioning

When Backups are enabled, Backup options are presented in the AUTOMATION tab of the provisioning wizard. Note that your default backup bucket and default backup schedule will be set according to your global backup settings as mentioned in the previous sections.

NOTE

The Backup options presented in the Automation tab can be disabled using a "Create Backup" Policy. See ../administration/policies/policies

BACKUP TYPE

Select the type for the Backup. Backup Types displayed will be filtered by available options for the selected Instance Layout

BACKUP NAME

Defaults to the Instance name

BACKUP TARGET

Select the Storage Provider target for the Backup (when applicable)

BACKUP JOB TYPE

Create a new job, clone an existing job, or Add to existing job

JOB NAME

Defaults to the Instance name

RETENTION COUNT

Maximum number of successful backups to retain

BACKUP SCHEDULE

Select the schedule for the backup job from the list of existing execution schedules

SYNTHETIC FULL (Currently only available for KVM VM Snapshot-type backups, such as those used with HVM Instances. More Layout types are expected to support synthetic full backups in the future)

When checked, an additional schedule is configured for the backup job during which a synthetic full backup will be taken. In general, this should be on a longer time period than that at which standard backups (full backup followed by incremental backups) are configured

SYNTHETIC FULL SCHEDULE

Select the schedule for the backup job on which synthetic full backups should be taken

Backup Types displayed will be filtered by available options per selected Instance Layout.

Summary

The Backups Summary section shows the following metrics:

- Number of Configured Backups trend
- Backup Success Rate
- Number of Completed Backups
- Number of Failed Backups
- Total Size of Backups (MB) trend
- Upcoming and In Progress Backups

If a User's Role permission for Backups is set to User, the user will only see metrics for backups they own.

Backups

In the Backups > Backups section, currently-configured Backups can be viewed and managed, and new Instance, Host and Provider backups be configured. Backups must be tied to a Backup Job, which holds the retention count and the schedule on which the backup should automatically be run. You can create a new Job at the same time as the backup is created or you can create the job ahead of time and associate any new backups to the existing job.

NOTE

Role permissions for Backups determine which backups will be accessible to the individual user.

Subtopics

Create an Instance Backup

Create an Instance Backup

About this task

To create Instance backup:

Procedure

1. Navigate to Backups > Backups
2. Click + ADD
3. From the Create Backup Wizard select the radio button for Instance, then click NEXT
4. Input the following:

   Instance

   Select an Instance to backup from the typeahead menu

   Name

   Enter a name for the backup job being created

5. Click NEXT
6. Depending on the Instance Type selected in the previous step, enter additional details. These can include a specific container, backup type, database name, username and password, or a number of other things depending on the Instance Type
7. Configure the storage bucket and retention details:

   Storage

   Select a configured storage bucket as the backup target

   Backup Job Type

   Create a new backup job, add this backup to an existing job, or clone an existing job to handle this backup

   Job Name

   If creating a new job, enter a name for the job

   Retention Count

   If creating a new job, enter the number of backups which should be simultaneously retained

   Schedule

   If creating a new job, select an execution schedule of which to run the backup

   Synthetic Full

   When the backup is targeting an HVM Instance, check this box to schedule synthetic full backups in addition to the normal full and incremental backups

   Synthetic Full Schedule

   If synthetic full backups are enabled, select an execution schedule on which to run the synthetic full backups
8. Click COMPLETE.

Results

NOTE

On VMware Cloud types, VM Essentials will merge and consolidate the snapshots held against a VM before exporting the OVF to the storage location or share. This is so VM Essentials has a full and consistent copy of the VM state.

TIP

To edit an existing backup, click on the hyperlinked name of the backup job from the list of backups at Backups > Backups.

Tools

Subtopics

Cypher
Archives
Migrations

Cypher

Subtopics

- Overview
- Mountpoints
- Creating Cypher Keys
- Password
- tfvars
- Secret
- UUID
- Key
- Vault
- Editing Cypher Keys
- Using Cypher Keys in Scripts

Overview

Cypher at its core is a secure Key/Value store. But what makes Cypher useful is the ability to securely store or generate credentials to connect to your Instances. Not only are these credentials encrypted but by using Cypher you don't have to burn in connection credentials between Instances into your apps.

Cypher keys can be revoked, either through lease timeouts or manually. So, even if somebody were to gain access to your keys you could revoke access to the keys and generate new ones for your applications.

Keys can have different behaviors depending on the specified mountpoint.

Mountpoints

password

: Generates a secure password of specified character length in the key pattern (or 15) with symbols, numbers, upper case, and lower case letters (i.e. password/15/mypass generates a 15 character password).

tfvars

: This is a module to store a tfvars file for terraform app blueprints.

secret

: This is the standard secret module that stores a key/value in encrypted form.

uuid

: Returns a new UUID by key name when requested and stores the generated UUID by key name for a given lease timeout period.

key

: Generates a Base 64 encoded AES Key of specified bit length in the key pattern (i.e. key/128/mykey generates a 128-bit key)

vault

: Configures an integration between VM Essentials and a Hashicorp Vault server. See below for additional configuration instructions.

- Key lease times are entered in seconds and default to 32 days (2764800 s).
  - Quick Time Reference:
  - Day: 86400
  - Week: 604800
  - Month (30 days): 2592000

- Year: 31536000

Creating Cypher Keys

Procedure

1. Navigate to Tools > Cypher and select + ADD
2. Configure one of the following types of Keys:

Password

A Cypher password generates a secure password of specified character length in the key pattern (or 15) with symbols, numbers, upper case, and lower case letters (i.e. password/15/mypass generates a 15 character password).

Key

Pattern “password/character_length/key”

Example: password/10/mypassword

Value

Leave the Value filed blank for a password, as it will be generated.

Lease

Enter lease time in seconds (ex. 604800 for one week)

Save changes and the password will be generated and available for use.

If your user role has Cypher: Decrypt permissions, a “DECRYPT” button will be available in the Cypher section to view the generated password.

To delete the password key, select Actions > Remove and confirm.

tfvars

A mountpoint to store tfvars files for Terraform App Blueprints.

Key

Pattern “tfvars/key”

Example: tfvars/my-aws-account

Value

The values for your tfvars file to be encrypted

Lease

Enter lease time in seconds (ex. 604800 for one week)

Click SAVE CHANGES and the stored values will be available for use.

NOTE

You may also see Cloud profiles stored at the tfvars mountpoint. They will have a key pattern like: “tfvars/profile/cloud/$cloudCode/variables”. Terraform Cloud profiles are created on the Cloud detail page (Infrastructure > Clouds > selected Cloud) under the Profiles tab. They allow Terraform apps and specs to be provisioned across multiple Clouds that require differed tfvars. See the **Cloud profiles** page for more.

Secret

A Cypher secret is the standard secret module that stores a key/value in encrypted form.

Key

Pattern “secret/key”

- EXAMPLE: secret/mysecret

Value

Add the secret value to be encrypted

Lease

Enter lease time in seconds (ex. 604800 for one week)

Save changes and the secret will be encrypted and available for use.

If your VM Essentials user role has Cypher: Decrypt permissions, a “DECRYPT” button will be available in the Cypher section to view the secret.

To delete the secret, select Actions > Remove and confirm.

UUID

A Cypher UUID Returns a new UUID by key name when requested and stores the generated UUID by key name for a given lease timeout period.

Key

Pattern “uuid/key”

- Example: uuid/myuuid

Value

Leave the Value filed blank for UUID, as it will be generated.

Lease

Enter lease time in seconds (ex. 604800 for one week)

Save changes and the UUID will be generate and available for use.

If your user role has Cypher: Decrypt permissions, a “DECRYPT” button will be available in the Cypher section to view the generate UUID.

To delete the UUID, select Actions > Remove and confirm.

Key

A Cypher Key generates a Base 64 encoded AES Key of specified bit length in the key pattern (i.e. key/128/mykey generates a 128-bit key).

Key

Pattern “key/bit_length/key”

- Example: key/256/mykey

Value

Leave the Value filed blank for key, as it will be generated.

Lease

Enter lease time in seconds (ex. 604800 for one week)

Save changes and the AES Key will be generate and available for use.

If your user role has Cypher: Decrypt permissions, a “DECRYPT” button will be available in the Cypher section to view the generate AES Key.

To delete the UUID, select Actions > Remove and confirm.

Vault

Use this mountpoint to store Cypher secrets in a Hashicorp Vault server backend rather than VM Essentials. Additionally, you can call secrets stored in Vault from this Cypher mountpoint even if they are only saved there and not listed in the VM Essentials Cypher UI. This requires installation and configuration of the Hashicorp Vault plugin. See the YouTube video embedded in this section for more information on adding the plugin, configuration, and a demonstration of its capabilities.

NOTE

It’s recommended that you use a long-lived token as attempts to call Vault-stored values into Tasks will stop working if the token is no longer good. In such a case you’d have to obtain a new token, delete the Cypher entry with the old token, and create a new one to restore functionality once again. Using a long-lived token will prevent the need to do this often.

Key

Pattern “vault/<engineMount>/<secretPath>/data/<key>” (ex. vault/KV2/secret/data/morpheus/lab)

Value

Enter your key/value pair here in valid JSON (ex. {“hello”: “world”})

Lease

Enter lease time in seconds (ex. 604800 for one week)

Click SAVE CHANGES. The example BASH script below onboards the value stored in Vault from the secret/data/morpheus/lab mountpoint:

```
from_vault="<%= cypher.read('vault/KV2/secret/data/morpheus/lab') %>"
echo $from_vault
```

Editing Cypher Keys

Cypher key types which accept user-entered values (not generated values) are editable. To edit, click the “ACTIONS” button at the end of the row for the appropriate Cypher key and then click “Edit.” Edit the values and click SAVE CHANGES.

Using Cypher Keys in Scripts

To use a Cypher key in a script, use the following syntax:

`<%=cypher.read('var_name')%>`

Example: `PASSWORD=<%=cypher.read('secret/myuserpassword')%>`

Cypher also includes an option to read a value from the `password/*` mountpoint or create one if it doesn't already exist. Use the following syntax:

`<%=cypher.readPassword('var_name')%>`

Example: `PASSWORD=<%=cypher.readPassword('myuserpassword')%>`

It should be noted that when Cypher keys are created using the `readPassword` function, the subsequent reads can only come from the same user. If another VM Essentials user attempts to run the automation script containing the `readPassword` call, the secret value will not be read and it's very likely the script will fail. For Tasks that need to be run by multiple users, use a pre-existing Cypher key and reference it back in the script using `read` rather than `readPassword`.

Archives

Subtopics

- Overview
- Archives List Page
- Adding an Archive
- Archive Detail Page
- File Detail Page

Overview

Archives provides a way to store your files and make them available for download by your scripts and Users. Archives are organized by buckets and can be tied to any existing Bucket or File Share that may be currently integrated (for more on integrating new storage targets, see storage documentation). Thus, storage buckets in public clouds, on networked storage, or even on the appliance itself may be used to host files.

Archives List Page

To view or create Archives, navigate to Tools > Archives. At the Archives list page is a list of all currently-configured Archives. From the list view, the following details about each Archive are shown:

- **NAME:** The name for the Archive in VM Essentials
- **BUCKET:** The integrated bucket or file share where files in this Archive are stored
- **# Files:** The number of files in the Archive
- **SIZE:** The total size of all files in the Archive
- **TENANTS:** When Archive visibility is set to Private, only the Tenants listed here have access to the Archive
- **VISIBILITY:** Public or Private, public Archives are available in all Tenants
- **PUBLIC URL:** Indicates whether VM Essentials is automatically generating a public download URL for files in this Archive
- **ACTIONS:** Within the ACTIONS menu users may download a ZIP folder containing all files in the Archive, edit the Archive, or remove it

Adding an Archive

To add a new Archive, click + ADD from the Archives list page. Configure the following:

- **NAME:** A friendly name for the Archive in VM Essentials
- **DESCRIPTION:** An optional description for the Archive
- **BUCKET:** Select an existing bucket or file share to store files in for this Archive. To integrate a new bucket or file share to use for an Archive, navigate to Infrastructure > Storage
- **VISIBILITY:** Public or Private, public Archives are available in all Tenants
- **TENANTS:** When Archive visibility is set to Private, only the Tenants selected will have access to the Archive
- **PUBLIC URL:** When marked, VM Essentials will create a public download URL for all files in the Archive

> **WARNING**
> Be sure that no sensitive data will be stored in the Archive if it will be configured to generate public URLs. Anyone with the public URL will be able to download the file without authentication.

Once done, click SAVE CHANGES

Archive Detail Page

The Archive detail contains information about the Archive configuration as well as a list of files currently stored in the Archive. The Archive detail is accessed by navigating to the Archives list page (Tools > Archives) and selecting an existing Archive. As on the Archives List Page, users can download a ZIP folder containing all files in the Archive and edit the Archive from the ACTIONS menu.

To delete the Archive, click DELETE. New files are added by clicking + ADD. When adding a new file, users may browse the file system on the local computer to select a file.

From the files list, download or delete individual files by clicking on the appropriate selection from the ACTIONS menu.

File Detail Page

The File Detail Page contains details about the file itself as well as private and public (if available) URLs. In the lower section are three tabs. The Links tab contains any download links which have been generated (both active and expired). The History tab contains historical information about the file including creation and deletion of download links and download events. The scripts tab contains a guide for getting started using Archive-stored files in scripts.

Migrations

Subtopics

Overview
Migrations Requirements
Migrations Plans
Configuring Windows Workloads (Windows 2022 or later) for Migration
Migrating a Windows VM (Online procedure)

Overview

The bulk migration tool is designed to migrate existing VMs running on integrated VMware vCenter Clouds to HVM Clusters. Thus, creating a migration requires existing vCenter Cloud integration(s) and at least one functional HVM Cluster. See the VMware vCenter integration guide and the HVM Clusters guide elsewhere in this documentation stack for more details on getting started with and using those integrations. Migrations may include multiple VMs and may include both Linux and Windows workloads.

Migrations Requirements

This section contains requirements and recommendations that will ensure migrations run successfully. Keep an eye on this section as some requirements will change as this feature is updated over time to become more flexible.

General Requirements

- HVM Hosts must be upgraded to Agent version 2.10.0 at minimum. To upgrade the HVM Host Agent, navigate to the host detail page, open the ACTIONS menu, and select "Upgrade Agent." If this is unsuccessful, you may instead select "Download Agent Script" to download a shell script which may be run manually on the HVM Host. These download scripts are specific to the HVM Host so an individual install script would need to be downloaded for each HVM Host and run on the correct HVM Host.
- HVM Hosts must be able to reach ESXi hosts and vCenter on the target VMware vCenter Cloud via the Management Network
- The source VMs must be running for the preparation phase of the migration to complete successfully. If VMs are not running, they will automatically be restarted

First Release Requirements

This section includes requirements for the current version of the migration feature which are subject to change and improvement as road-mapped enhancements are included with subsequent versions of the product.

- The destination datastore must have enough "thick" space for each VM
- VMs will power down prior to the transfer meaning service of the source workload will be disrupted during the transfer
- VirtIO / VirtIO-SCSI target storage must be supported by the source VM
- Currently supported operating systems: RedHat, CentOS, Rocky, Alma, SUSE, Ubuntu, Debian, Windows (currently requires manual preparation steps described below)
- Source VMs must be capable of getting the `qemu-guest-tools` package installed via package managers (yum, apt, dnf, zypper). If they are not, this can be manually performed by setting the "skip guest tools" flag on the migration
- RDM (Raw Device Mappings) are not yet supported
- Source VMs must not have any attached ISOs or cdroms. These are not supported and the migration will fail.

Recommendations

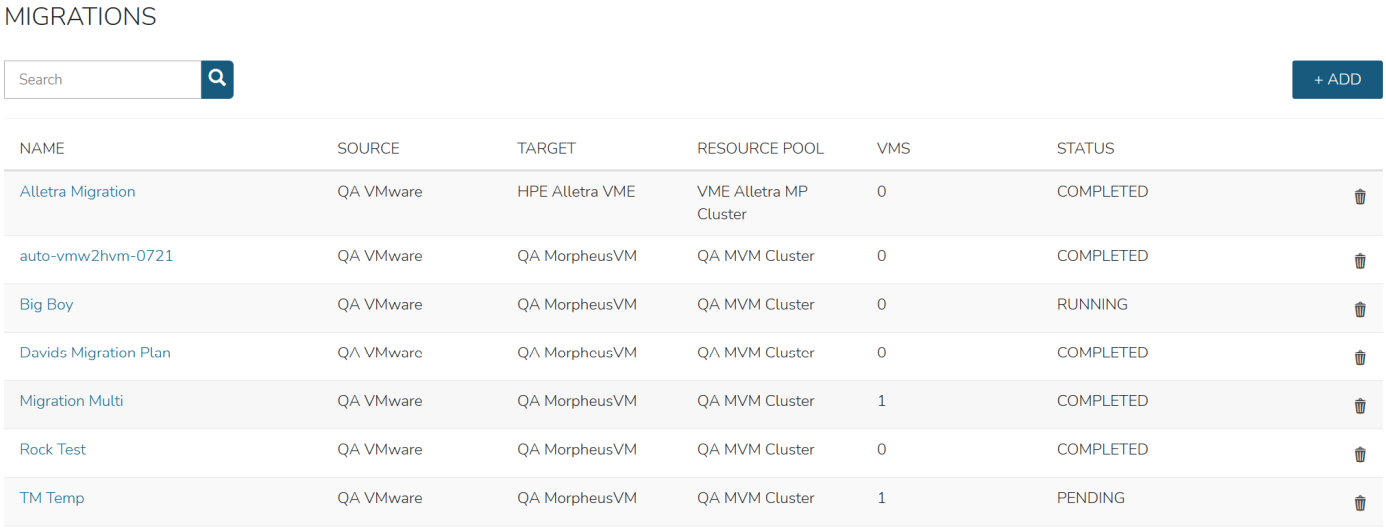
- Batch limits and bandwidth limitations testing is still in progress. It's currently recommended you migrate no more than 20 VMs at a time. Testing is still ongoing to determine the upper limits of migrations and this recommendation is likely to increase over time
- Begin using this feature with a smaller migration than the limit to make sure your workloads are moving correctly

Migrations Plans

Migration plans are created and run from the Migrations section of the Tools menu (Tools > Migrations). Migrations happen by creating and running Migration Plans. Plans are created in a pending state, meaning an additional action must be undertaken to set the plan in motion. Thus, Plans may be created which are intended to be run at a later time. Once finished, completed Plans remain on the Migrations list page for later review and, if desired, deletion.

Creating Migration Plans

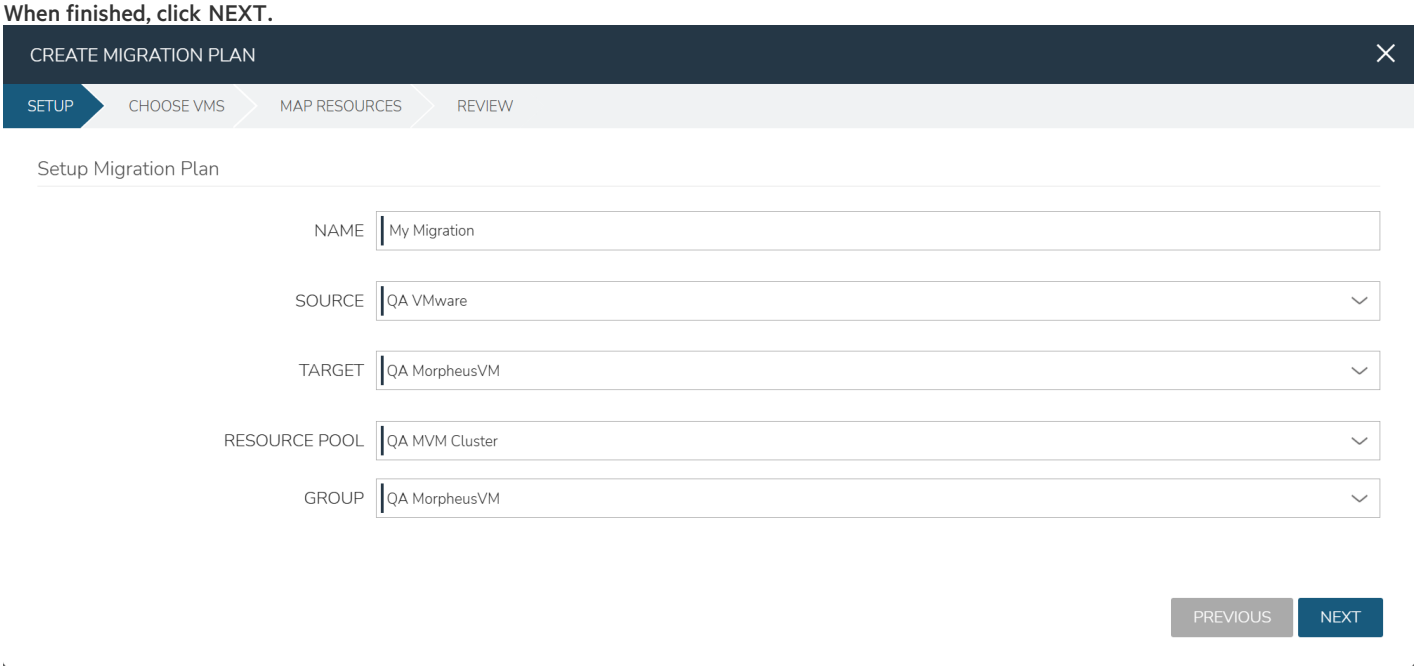
Begin creating a Migration Plan from the Migrations list page (Tools > Migrations). This page contains a list of all Migrations already created, including those completed, currently running, and available to be run (pending). To start a new Migration, click + ADD.



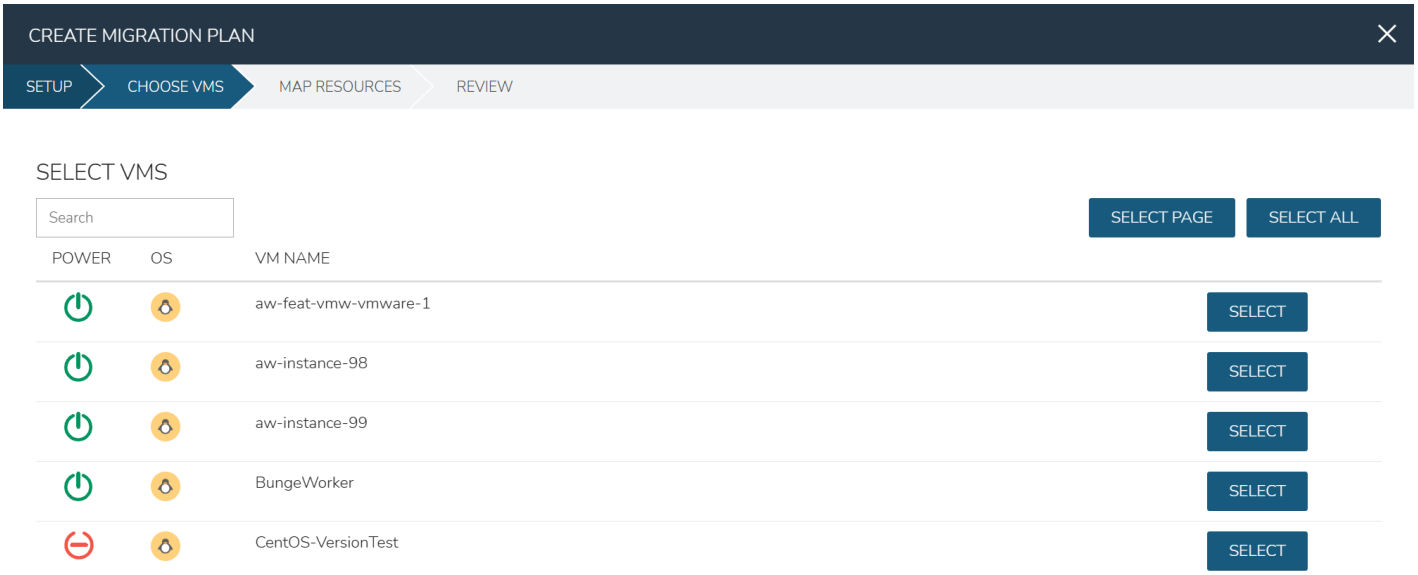
From the SETUP tab of the CREATE MIGRATION PLAN modal, configure the following:

- **NAME:** A name to identify the Migration
- **SOURCE:** The source VMware vCenter Cloud
- **TARGET:** The target Cloud containing the HVM Cluster
- **RESOURCE POOL:** The selected destination HVM Cluster
- **GROUP:** The Group which should own the migrated VMs

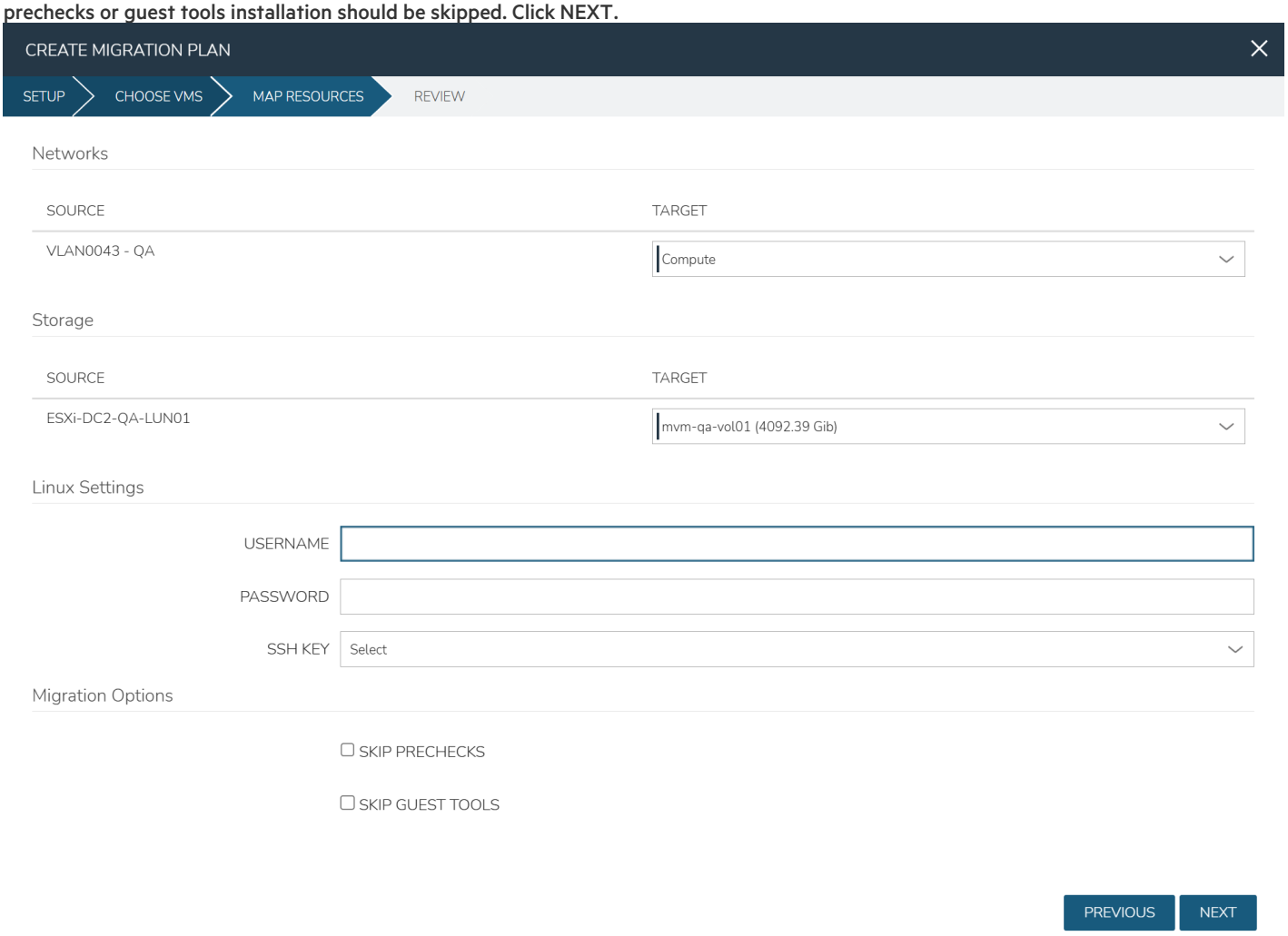
When finished, click NEXT.



The next step is to choose VMs from the selected VMware source Cloud to migrate. Select as many as desired given current recommendations regarding the maximum size due to storage space and available bandwidth (see the previous section). Selected VMs will form a list at the bottom of the modal. When finished, click NEXT.



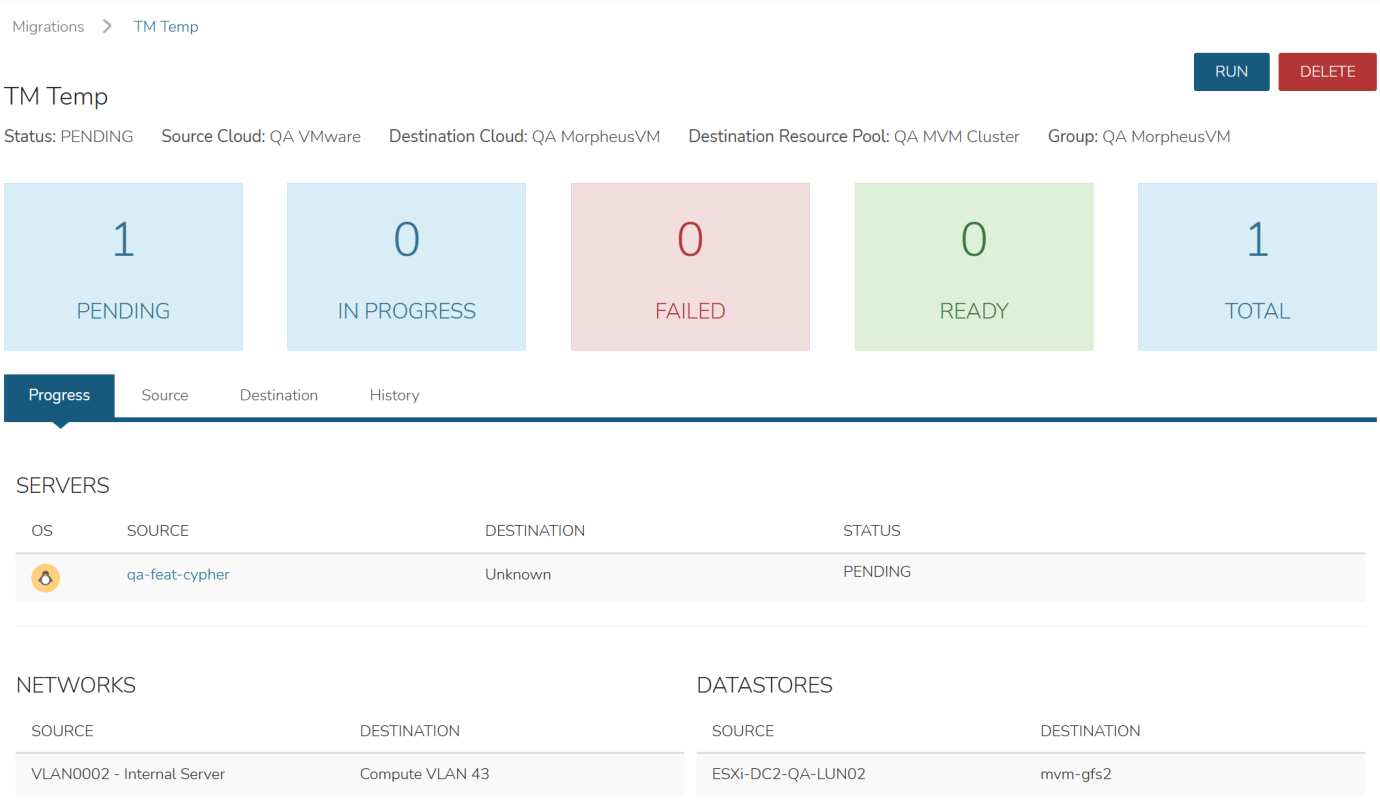
The next tab establishes resource mapping. Listed, you will see the current networks and storage locations for the selected VMs. Choose destination networks and destination storage locations for each. Optionally, enter existing Linux or Windows user credentials and choose if prechecks or guest tools installation should be skipped. Click NEXT.



The final tab is a review tab where all current selections can be checked. Return to any previous tabs, if necessary, to update selections.

At this point, the Migration is created but will not run without additional input. The Migration is in a "Pending" state. All selections made when configuring the Migration are shown here. To execute the Migration, click RUN. The length of time it will take for the Migration to run depends on many factors. Once run, the Migration detail page will provide status updates on VMs currently being migrated, which have completed successfully, and if any have failed. The History tab provides greater detail on current and past migration actions taken. The

Destination tab includes details on VMware VMs which have successfully been migrated to the HVM Cluster. Migrations are run just once and may be kept indefinitely after for review. When a Migration is no longer needed, click DELETE.



Configuring Windows Workloads (Windows 2022 or later) for Migration

Migrating Windows workloads from VMware vCenter Clouds to HVM Clusters using the bulk Migrations feature requires some initial configurations checks. This section goes through an example preparation process for a Windows VM running on vCenter.

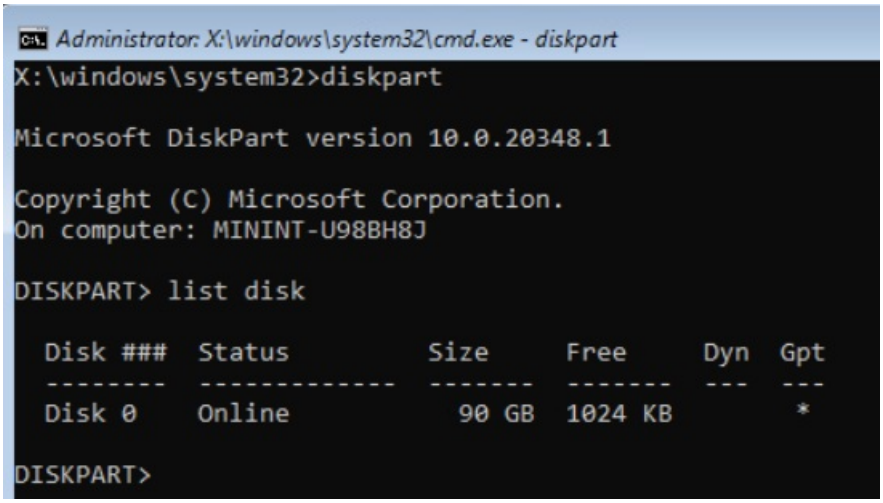
This guide makes the following assumptions about the workload to be migrated:

- Configured to boot as EFI or BIOS
- Virtualization Based Security (VBS) is enabled
- Secure Boot is enabled
- Trusted Platform Module (TPM) is disabled
- The VM has access to the recovery partition (if not, a Windows Recovery Environment disc or installation media may be required to access some of the menus referenced in this section)

Inject VirtIO Drivers

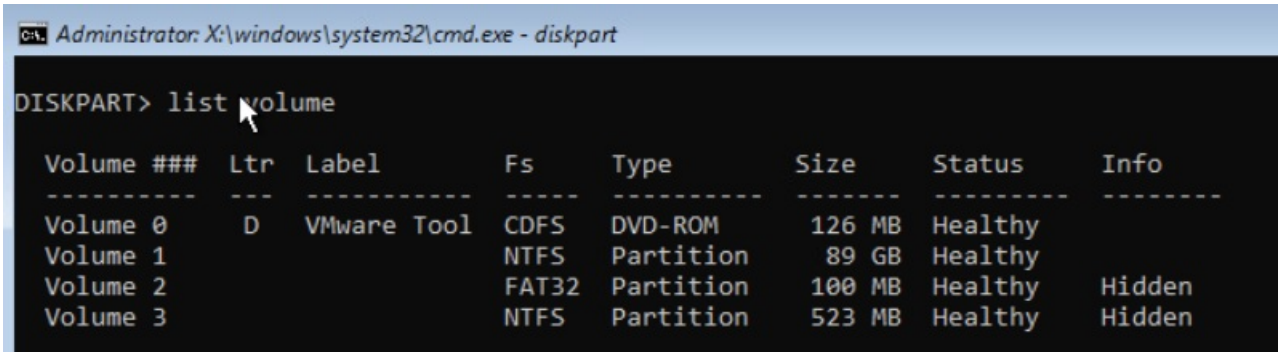
To begin, restart the VMware Windows guest in the **Windows Recovery Environment (Windows RE)**. In Windows RE, choose a keyboard layout if prompted. Then, select the **Troubleshoot** option. From the Troubleshoot menu, select **Command Prompt**.

Within the Command Prompt session, enter **diskpart** using this command: `diskpart`. Check the disks that are available with `list disk`. At this point, you may receive the message that "There are no fixed disks to show." or the disk with Windows OS might not be listed. If that is the case, follow the steps in the next section to mount the drives. If that is not the case, skip to the following section to continue the process of injecting the VirtIO drivers.



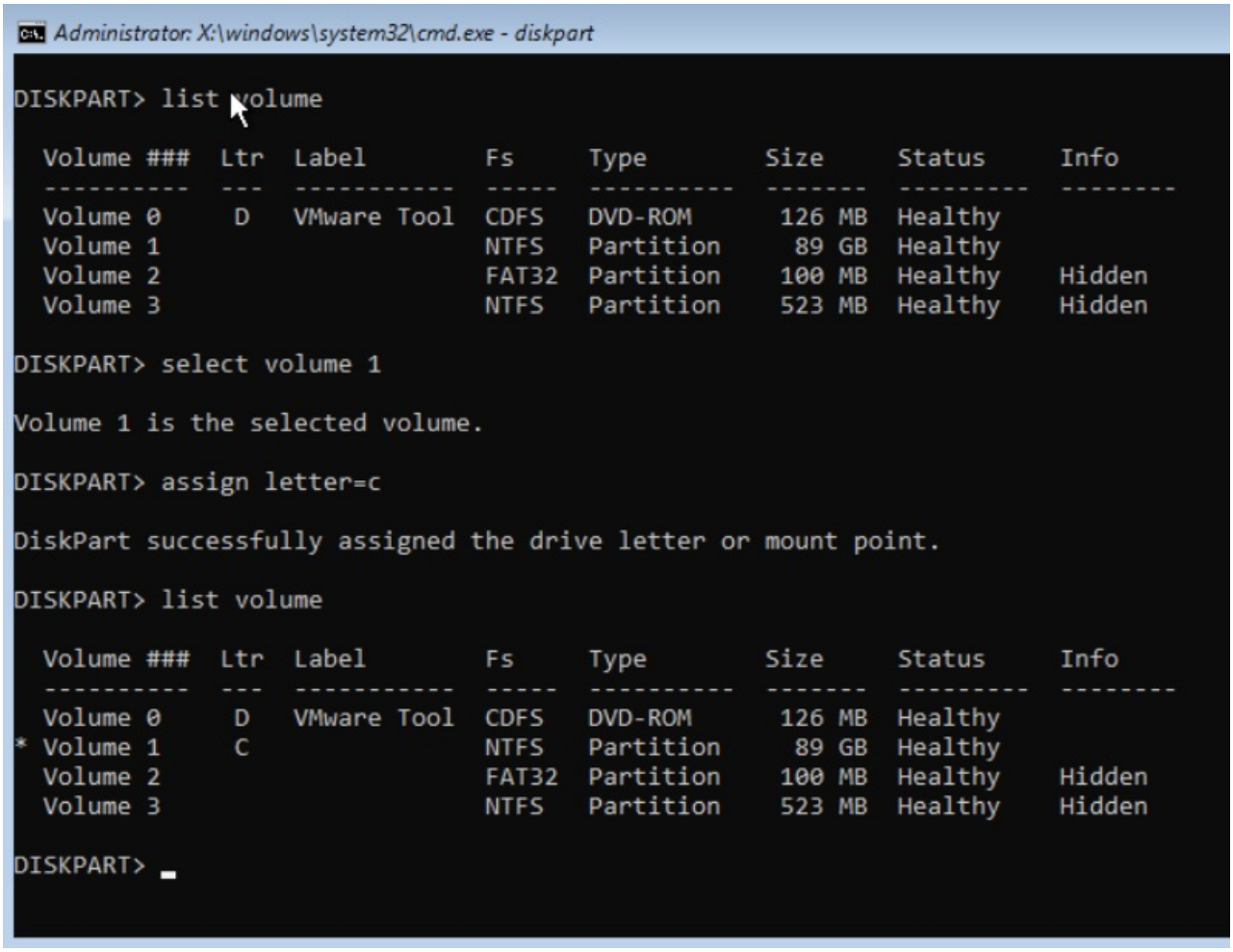
Mounting the Drives

From vCenter, mount the VMware Tools installer to the VM using the "Install VMware Tools..." option (**Actions > Guest OS > Install VMware Tools...**). Then, back in diskpart, use the following command to find the CD/DVD-ROM drive letter: `list volume`. Make note of the CD-ROM drive letter, which in the case of this example is drive "D." Exit diskpart with the `exit` command.


Administrator: X:\windows\system32\cmd.exe - diskpart
DISKPART> list volume
Volume ### Ltr Label Fs Type Size Status Info
Volume 0 D VMware Tool CDFS DVD-ROM 126 MB Healthy
Volume 1 NTFS Partition 89 GB Healthy
Volume 2 FAT32 Partition 100 MB Healthy Hidden
Volume 3 NTFS Partition 523 MB Healthy Hidden

Enter the following command to load the storage drivers which will enable you to see the hard disks: `drvload "D:\Program Files\VMware\VMware Tools\Drivers\pvscsi\Win10\amd64\pvscsi.inf"`. Note that the prior command references Windows 10 as the operating system but choose the most appropriate or the latest available. It also references drive "D" which may vary from case to case.

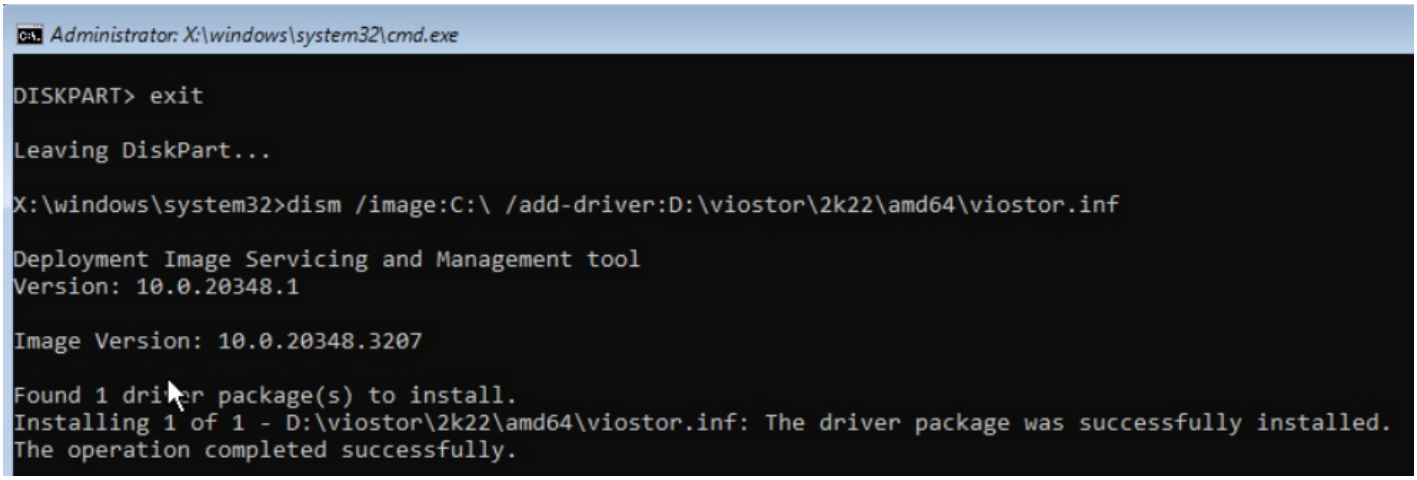
With the driver loaded, once again confirm the disks are mounted with `diskpart` and `list disk`. They're now mounted but the partitions/volumes need drive letters so, while still in diskpart, list the volumes with: `list volume`. In this example case, "Volume 1" is the primary Windows volume. Select the volume and assign a drive letter, in the example case the assigned letter will be "C": `select volume 1` and `assign letter=c`. Check your work by listing the volumes again, the primary Windows volume should be assigned the correct drive letter: `list volume`.


Administrator: X:\windows\system32\cmd.exe - diskpart
DISKPART> list volume
Volume ### Ltr Label Fs Type Size Status Info
Volume 0 D VMware Tool CDFS DVD-ROM 126 MB Healthy
Volume 1 NTFS Partition 89 GB Healthy
Volume 2 FAT32 Partition 100 MB Healthy Hidden
Volume 3 NTFS Partition 523 MB Healthy Hidden
DISKPART> select volume 1
Volume 1 is the selected volume.
DISKPART> assign letter=c
DiskPart successfully assigned the drive letter or mount point.
DISKPART> list volume
Volume ### Ltr Label Fs Type Size Status Info
Volume 0 D VMware Tool CDFS DVD-ROM 126 MB Healthy
* Volume 1 C NTFS Partition 89 GB Healthy
Volume 2 FAT32 Partition 100 MB Healthy Hidden
Volume 3 NTFS Partition 523 MB Healthy Hidden
DISKPART>

Exit diskpart once again (`exit`) and unmount the VMware Tools installer from the VM back in the vCenter console (**Actions** > **Guest OS** > **Unmount VMware Tools Installer**).

Inject VirtIO drivers (cont.)

Download the **latest** or **stable** VirtIO drivers ISO to your local workstation. The latest is recommended but often they are the same. Add the ISO to vCenter either by uploading it to a datastore or to the Content Library. Still in vCenter, mount the ISO using a CD-ROM device on the VM and make sure it's connected. Enter the following commands to inject the VirtIO storage drivers into the Windows boot-start drivers from the mounted ISO: `dism /image:C:\ /add-driver:D:\viostor\2k22\amd64\viostor.inf` and `dism /image:C:\ /add-driver:D:\vioscsi\2k22\amd64\vioscsi.inf` . Note once again that the OS volume will not be assigned the "C" drive letter and the CD-ROM device will not be assigned the "D" drive letter in every case. Similarly, in this example "2k22" is used but that won't be appropriate in every case. If successful, a message will be received that the driver packages were successfully installed. Close the Command Prompt window and click **Continue** to boot Windows once again.


Administrator: X:\windows\system32\cmd.exe
DISKPART> exit
Leaving DiskPart...
X:\windows\system32>dism /image:C:\ /add-driver:D:\viostor\2k22\amd64\viostor.inf
Deployment Image Servicing and Management tool
Version: 10.0.20348.1
Image Version: 10.0.20348.3207
Found 1 driver package(s) to install.
Installing 1 of 1 - D:\viostor\2k22\amd64\viostor.inf: The driver package was successfully installed.
The operation completed successfully.

```
X:\windows\system32>dism /image:C:\ /add-driver:D:\vioscsi\2k22\amd64\vioscsi.inf

Deployment Image Servicing and Management tool
Version: 10.0.20348.1

Image Version: 10.0.20348.3207

Found 1 driver package(s) to install.
Installing 1 of 1 - D:\vioscsi\2k22\amd64\vioscsi.inf: The driver package was successfully installed.
The operation completed successfully.

X:\windows\system32>_
```

Prepare the OS

Once logged back in, install the VirtIO drivers in the OS using the ISO, which is still mounted, by navigating to the CD-ROM/DVD-ROM drive. Install `virtio-win-gt-x64.msi` and `virtio-win-guest-tools.exe` from the root of the ISO. Maintain all default selections during the installation. Next, unmount any ISOs still attached to the VM, either by ejecting in Windows or by setting the CD-ROM drive to "Client Device" in vCenter.

Now, shut down the VM. Keep in mind that the VMware Cloud integration may be configured to automatically maintain power state of associated VMs. Navigate to Infrastructure > Clouds and edit the Cloud. Make note of the "AUTOMATICALLY POWER ON VMS" configuration. If checked, you will need to shut down the VM via the product UI tools rather than from the vCenter console or from within the guest OS. Alternatively, you could uncheck "AUTOMATICALLY POWER ON VMS", save changes to the Cloud, and then power down the VM from vCenter or from the guest OS but bear in mind changing this configuration would affect all VMs associated with the Cloud in the product.

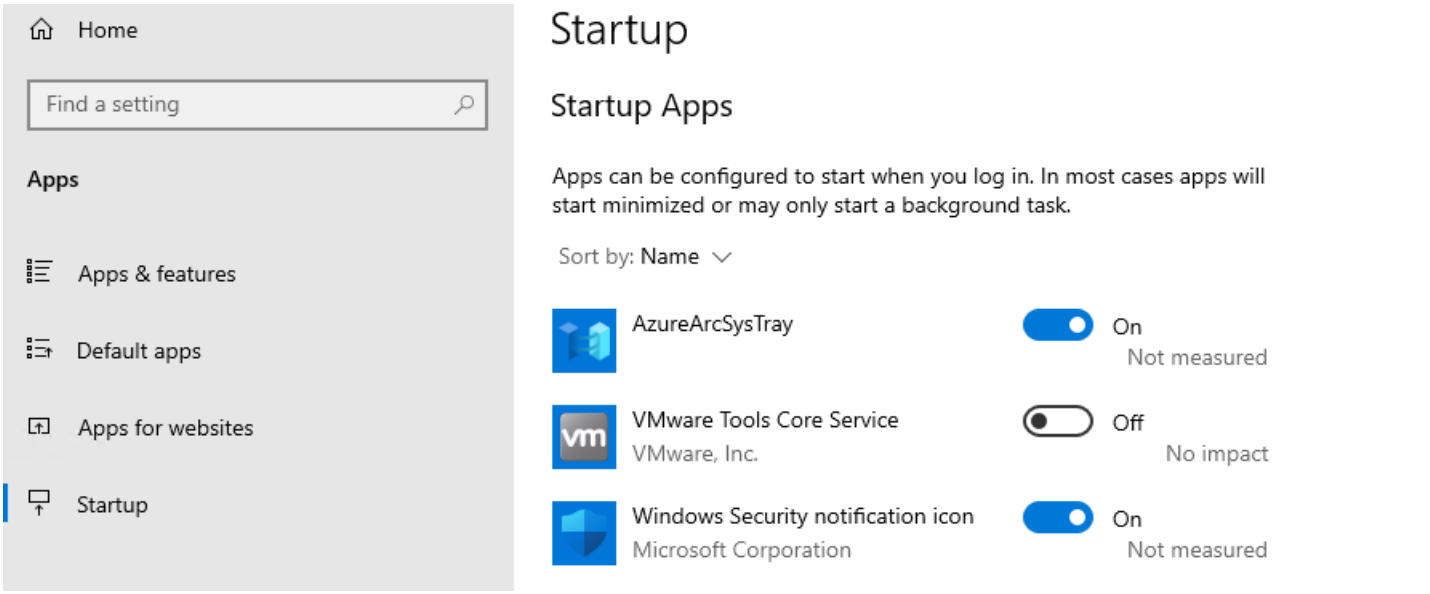
Migrating

This completes the preparation steps. From here, create a new Migration Plan that includes the prepared VM and run it. Take a look at the previous section for more information on creating and running Migration Plans.

Post-Conversion

As a final note, bear in mind that the migration tool does not uninstall VMware Tools following conversion, which can lead to start-up errors being surfaced in migrated VMs. In some cases, the VMware Tools installation may become corrupted which prevents simply uninstalling using the Control Panel.

To prevent VMware Tools from executing at startup, within the Windows guest navigate to Settings > Apps > Startup and turn off VMware Tools Core Service. See the example screenshot below for a Windows 2022 Guest.



Additionally, you can attempt to uninstall VMware Tools completely using Microsoft recommended processes and tooling for uninstalling stuck programs. See this article from the Microsoft Support for procedure and links to a helpful tool.

Migrating a Windows VM (Online procedure)

Migrating a Windows VM (Offline procedure)

About this task

This procedure includes steps to migrate the VM without having to utilize the WinRE mode to inject drivers.

Procedure

1. Log in to the VM using the admin credentials.
2. Download the latest ISO drivers.
3. Mount the ISO.
4. Install appropriate windows .exe & .MSI software.
5. Browse to /amd64 folder. Right-click the **.INF** setup information file to install the appropriate SCSI and IOSTOR drivers and select **Install**.
6. Shutdown VM.
7. Migrate the VM using Migration tool within Morpheus.
8. Reconfigure the VM to boot to SATA0:0.
9. Boot the VM. After a few minutes the VM will be up and running.
10. Shut down the VM.
11. Reconfigure the VM to boot to SCSI0:1.
12. Boot the VM. After a few minutes the VM will be up and running.

Administration

There are several administrative integrations built into VM Essentials that make it great to work with within any organization ranging from small to large. Especially, with its built in white label support and multitenancy capabilities, managed service providers have a wide range of capabilities when it comes to managing customer accounts and users.

Subtopics

- Identity Sources
- Plans & Pricing
- Roles
- Users
- Health
- Settings
- User Settings

Identity Sources

Administration > Tenants > (Selected Tenant) > Identity Sources Administration > Users > Identity Sources

Subtopics

- Overview

Overview

VM Essentials can integrate with many of the most common identity source technologies, such as Active Directory, Okta, and many others. These can be configured via the Identity Sources button on the Users list page (Administration > Users). These integrations map roles within these sign-on tools to equivalent roles in VM Essentials so at first log in users are assigned the appropriate role.

Plans & Pricing

Subtopics

- Overview

Overview

Service Plans determine the amount of compute resources available to each Instance. When provisioning new Instances from VM Essentials, a plan is selected which determines the number of CPU cores, amount of memory and the amount of storage available to the associated machines. Additionally, when converting discovered instances in integrated clouds to VM Essentials-managed Instances, the user selects a plan which best fits the instance as it is currently configured. When Instances are reconfigured, a new plan may be selected which redefines the compute resources which should be available to the Instance. Plans can be as specific or open-ended as the user would like, restricting the user to the resources defined in the plan or allowing the user to increase those amounts at provision time.

The Plans section (Administration > Plans & Pricing) is where Plans are managed. A set of Service Plans are seeded by VM Essentials for immediate use with supported Cloud type out of the box. Additional Plans may be synced in on integrating additional Clouds depending on the type. Users can create new Service Plans or edit the system-seeded Service Plans for Private Cloud types.

Subtopics

- Create Service Plan
- Service Plan Permissions
- Service Plan Configuration

Create Service Plan

About this task

Price Sets can be added to the Plan at creation time so often it makes sense to create the Prices and associate them with Price Sets before creating the Plan. Additional instructions for creating Prices and Price Sets are in the next section. With the Price Sets ready, continue with the instructions below to create Price Plans of various types.

Procedure

1. Navigate to Administration > Plans & Pricing (`/admin/service-plans`)
2. Click the + ADD dropdown and select the appropriate Plan type
3. Configure details for the Plan on the General tab, the configuration options will depend on the Plan type. See the section above for a detailed description of each configuration option available for Service Plans
4. On the Price Sets tab, associate all relevant Price Sets with the Plan. The desired Price Sets must already exist. If needed, you may save the Plan at this point and come back to associate Price Sets later
5. Click SAVE CHANGES

Service Plan Permissions

Group Access permissions determine availability of a Service Plan to Users based on their associated Roles.

- Group Access determines which Groups the Service Plan will be available in for Provisioning and Reconfigure.

Service Plan Configuration

NOTE

Not all fields listed below are available for every provision type. After selecting the provision type, the correct fields for that type of Service Plan will be revealed. Not all fields are required to save a valid Service Plan

- **NAME:** The name of the Service Plan in VM Essentials
- **ACTIVE:** Inactive Service Plans are not available for selection during provisioning or reconfigure. New discovered records cannot be associated with deactivated Plans when converting to managed resources. Any resources attached to a Plan will continue to be associated if the Plan is later deactivated
- **CODE:** A unique identifier for use in VM Essentials API and CLI
- **DISPLAY ORDER:** Configures the order in which plans are displayed relative to other plans associated with the same provision type. Note that Plans will be displayed in low-to-high order based on the Display Order property. This is reversed from Layouts which are displayed in high-to-low order
- **PROVISION TYPE:** Determines the resource Provision Type this Service Plan is available for when provisioning, reconfiguring and converting discovered resources to managed
- **REGION CODE:** (Optional) Limits availability of the Service Plan to Clouds with the specified Region Code
- **STORAGE:** The default storage size of the root volume (in MB or GB)
- **CUSTOMIZE ROOT VOLUME:** Allows the root volume size to be customized during provisioning or reconfigure. Custom Range limits, if set, will apply
- **CUSTOMIZE EXTRA VOLUMES:** Allows the extra volume sizes to be customized during provisioning or reconfigure. Custom Range limits, if set, will apply
- **ADD VOLUMES:** Allows additional volumes to be added during provisioning or reconfigure
- **MEMORY:** The amount of memory included with the plan (in MB or GB)
- **CUSTOM MEMORY:** Allows the amount of memory to be customized during provisioning or reconfigure. Custom Range limits, if set, will apply
- **CORE COUNT:** The number of virtual CPU cores included with the plan
- **CUSTOM CORES:** Allows the number of virtual CPU cores to be customized during provisioning or reconfigure. Custom Range limits, if set, will apply
- **CORES PER SOCKET:** Determines core distribution across sockets. CORES PER SOCKET cannot be larger than CORE COUNT, and CORE COUNT must be divisible by CORES PER SOCKET. For example four CORES with two CORES PER SOCKET means two sockets would have two cores each assigned. Four CORES with one CORE PER SOCKET would have four sockets with one core each assigned, and four CORES with four CORES PER SOCKET would have one socket with four cores assigned
- **TOTAL STORAGE:** When custom storage is enabled for the plan, this sets a minimum and maximum total storage allowed (all disks combined)
- **PER DISK SIZE:** When custom storage is enabled for the plan, this sets the minimum and maximum storage for each disk
- **CUSTOM MEMORY RANGE:** The minimum and maximum allowed amount of memory for the Plan when CUSTOM MEMORY is enabled for

the Plan

- **CUSTOM CORES RANGE:** The minimum and maximum allowed amount of virtual CPU cores for the Plan when CUSTOM CORES is enabled for the Plan
- **SOCKETS:** The minimum and maximum allowed sockets range for the Plan when CUSTOM CORES is enabled for the Plan
- **CORES PER SOCKET:** The minimum and maximum allowed cores per socket for the Plan when CUSTOM CORES is enabled for the Plan
- **PRICE SETS:** In the Price Sets tab, associate Price Sets with the Plan. See Adding Price Sets to Plans

TIP

Custom Range storage and memory values units (GB/MB) are inherited from the :STORAGE:: and :MEMORY:: GB/MB settings in the same Plan. For example, if :STORAGE: is configured for for 40 GB, a custom range for Storage would also be in GB.

Roles

Subtopics

Overview
Roles and Identity Sources
Role Permissions

Overview

Within VM Essentials is a wide array of role-based access control capabilities. These roles can be managed within the Administration > Roles section of the VM Essentials UI as well as through the API or CLI. Entire sections within the appliance UI can be hidden based on the specified access levels for features within VM Essentials. Features have different access scopes that can be selected from and can range depending on the specific feature. The most common scope set involves none, read, and full.

There are several handy tricks for creating new roles within VM Essentials and users can be assigned more than one role. When a user is assigned more than one role, permissions are granted by the role with the highest level of scope access. This allows roles to be built with small subsets of features and combined to grant different individuals relevant permission control. With resource permissions (that is, all types of permissions other than Feature permissions), a default access can be given as opposed to a specific (Full or None) permission for any resource. A specific permission will always supersede a default permission regardless of whether it's more permissive or more restrictive. In other cases (default vs default OR specific vs specific) the more permissive access will be given.

It's also important to note that built-in Roles, such as the System Admin "Superuser" Role carry no special prominence. For resource permissions, the System Admin user has defaults set to Full in each section. Thus, pairing the System Admin Role with another Role that may include specific line item permissions for various resource categories may cause your System Admin users to take on a reduced permission set.

NOTE

Feature access control not only applies to the VM Essentials UI but also applies to the public developer API. It is sometimes necessary to logout and back in for changes to a users feature access level to be respected.

Subtopics

Role Creation

Role Creation

Roles are created within Administration > Roles. Creating a Role requires minimal information, just a Name for the Role in VM Essentials. You can optionally add a Description and a Landing URL as well. The landing URL determines the starting page for the User on initial login (such as the Instances list page or perhaps the detail page for a primary HVM cluster). Following creation, click into the Role from the Roles list page and you will see the granular controls available to Roles. These controls include access permissions for UI feature sections, Groups, Cluster types, and configured Tasks. Changes are automatically saved for the Role, there is no need to click a button to save any updates. See the next section for a detailed breakdown of individual feature permissions.

Master tenant users are able to create a special type of user role called a multi-tenant user role. A multi-tenant user role is copied / duplicated down to all subtenants within VM Essentials. These can be viewed as canned role templates available to new tenants when their account is first created. Any changes made to the main role are propagated down to the subtenants version of the shared role so long as the subtenant users have not previously adjusted/changed that role. The moment a subtenant makes adjustments to the shared role within their account, it is unlinked from the parent role and treated entirely independently. In order to relink the Role in the Subtenant, a Master Tenant user would have to edit the Role, uncheck MULTITENANT USER ROLE, save the Role, check MULTITENANT USER ROLE once again, then save the Role once again.

Another note about user roles is that when a user role is copied down to a subtenant, the permission scopes cannot supersede the tenant's assigned tenant role. If they do they are automatically downgraded when propagated to the specific tenant. Any changes made to the tenant role will automatically ensure roles within the tenant are downgraded appropriately.

Master Tenant administrators may edit permissions for Roles in other Tenants by viewing the Tenant detail page (Administration > Tenants > Selected Tenant) and accessing the Roles tab. From there, select the Role to edit and make changes on the resulting Role detail page.

Roles and Identity Sources

It is very common for large Enterprises to have an existing identity source that they would like to plug in to VM Essentials for authentication. This includes services like LDAP, Active Directory, OKTA, Jump Cloud, One Login, and SAML. When using these services it becomes important to configure a role mapping between the VM Essentials role assignments to the equivalent identity source groups/roles the user belongs to. This is configurable within the identity source management UI. Sections are provided allowing things like LDAP groups to be directly mapped to specific roles within VM Essentials. If a user matches more than one LDAP/role group then both sets of roles are applied to the user automatically. Configuring Identity Sources is done in Administration > Users. Additionally, administrators may opt to lock users to their mapped role in VM Essentials or keep the roles unlocked to manually administer roles in one-off scenarios. See the docs section dedicated to identity sources for more information on configuring the specific SSO technologies VM Essentials supports.

Role Permissions

NOTE

Permission options for sub-tenant user roles will only list options permitted by the Tenant role applied to the sub-tenant. Sub-Tenant user roles permissions cannot exceed permissions set by the overriding Tenant Role.

Subtopics

Role Permission Sections

Feature Access Permissions

Role Permission Sections

Features

Controls User access level for UI sections and features in VM Essentials. The complete feature permissions grid is included below.

Groups

Controls User access level for Groups. Groups are not a Multi-Tenant construct, only Groups created in the current Tenant will be visible.

Cluster Types

Controls user access to Cluster types. Only Cluster types allowed for the Role may be added in Infrastructure > Clusters (assuming the Role also has feature access to applicable permissions related to adding Clusters) VDI Pools

Controls User access to VDI Pools which are currently configured (Tools > VDI Pools) via the Virtual Desktops Persona view

Workflows

Controls User access to configured Workflows, including the ability to view, edit, execute, or apply to Library item configurations

Tasks

Controls User access to configured Tasks, including the ability to view, edit, execute, or apply to Workflows

Feature Access Permissions

Feature Access settings control permissions for sections and objects in VM Essentials. Permission options include:

None

Hidden or inaccessible for user

Read

User can view but cannot edit or create

Full

User has full access

User

User can access Objects they have created or own

Group

User can access Objects assigned to or shared with Groups the User has access to

Remote Console: Provisioned

Remote Console tab will only appear after instance is successfully provisioned.

Remote Console: Auto Login

RDP and SSH only, controls if user is auto-logged in to Remote Console or presented with login prompt.

Role Mappings

Gives User Access to Role Mappings config in `/admin/roles` for configuring Identity Source Role Mappings without providing Access to other Identity Source configuration settings.

Admin Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Admin: Ansible	None, Full	Allows or disallows the ability to edit existing Ansible integrations	Ansible integrations are shown on the Integrations list page (Administration > Integrations). Users with access may view and edit them here.	This permission is recommended for those responsible for administering VM Essentials, including creating integrations with third-party technologies, specifically Ansible	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Admin: Appliance Settings	None, Full	Allows or disallows access to the Appliance and License tabs in Administration > Settings	The Appliance tab in Administration > Settings is where VM Essentials administrators would configure the appliance URL, Tenant and User management, email, proxy, and currency settings. Additionally, defining which Clouds are available for integration within VM Essentials is done on this page. On the License tab information about the current VM Essentials license may be viewed and a new license may be applied when needed.	This permission is recommended to only be assigned to Roles utilized within the Master Tenant. Those responsible for configuring currency, email, and proxy settings for Cloud API access will need this permission.	This permission is recommended to be set to None on the Tenant Role to restrict this access for all Subtenant Users.
Admin: Backup Settings	None, Full	Allows or disallows access to Administration > Settings > Backups. Master Tenant administrators have additional settings for appliance backups and defaults on this page.	The Backup Settings page is where users define the default VM Essentials backup bucket, backup schedule, and retention count. Additionally, if given to a Master Tenant user they will have the ability to enable scheduled backups, create backups, and backup appliance.	This permission is recommended for those responsible for enabling backups and setting default backup buckets within VM Essentials.	
Admin: Clients	None, Full	Allows or disallows access to the Clients tab in global settings (Administration > Settings)	The Clients settings section is where API clients are created and edited. Default clients may have their validity and refresh periods edited but cannot be deleted. User-created API clients may be edited or deleted	This permission is recommended for those responsible for administering API access.	
Admin: Distributed Workers	None, Full	Allows or disallows access to Administration > Integrations > Distributed Workers Tab			
Admin: Environment Settings	None, Full	Allows or disallows access to the Environments tab in Administration > Settings > Provisioning. When given to a Master Tenant user they may define the visibility of the environment to either private or public. When given to a Subtenant user the environments are only visible to the subtenant (private).	The Environments tab is where named environments such as development or production are created and given a description as well as a code for use within the API. A display order and visibility is also set.	This permission is recommended for those responsible for defining environments that will be available to select at provision time whether they are the Master Tenant or Subtenant users.	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Admin: Export/Import	None, Full	Allows access to the Export/Import functionality which is part of the Code Repositories section of VM Essentials UI (Provisioning > Code)	Export/Import tools allow users to configure integrated Git repositories as either export or import targets (or both) and execute exports or imports	This permission is recommended for administrators as it allows wholesale export of VM Essentials constructs (Tasks, Library Items, and more) as code into Git repositories as well as import of new items from repositories into the appliance	
Admin: Guidance Settings	None, Full	Allows or disallows access to the Guidance tab in Administration > Settings	The Guidance tab controls global thresholds for VM Essentials guidance recommendations	This permission is recommended for those responsible for cost and resource management	
Admin: Health	None, Read	Determines access to the Administration > Health page, including the VM Essentials Health and VM Essentials Logs tabs.	The Health pages provide an overview of VM Essentials health, notifications from integrations, and the current VM Essentials-ui log.	This permission is recommended for those responsible for administering and troubleshooting VM Essentials.	This permission is recommended to be set to None on the Tenant Role to restrict access for Subtenant users.
Admin: Identity Source	None, Role Mappings, Full	Allows or disallows access to create, edit, or delete integrated Identity Sources associated with subtenants. The “Role Mappings” option allows the user to edit role mappings without seeing higher level details about the integration itself (such as server IP addresses and admin usernames).	The Identity Sources page associated with the selected Tenant allows for creating, editing, and removing of identity sources in addition to configuring role mapping between VM Essentials and the identity provider.	Full permission is recommended for those responsible for integrating VM Essentials with Identity Providers. Role Mapping permission is recommended for those responsible for Role Based Access Control (RBAC).	This permission is recommended to be set to None for any subtenant user roles via use of a Tenant Role unless they manage their own RBAC.
Admin: Integrations	None, Read, Full	This allows or disallows full or read access to Administration > Integrations.	The Administration Integrations tab is where many new or existing integration types can be configured. These include Chef, Puppet, Ansible, Ansible Tower, vRealize Orchestrator, Microsoft DNS, PowerDNS, Route 53, Git, GitHub, Docker, Jenkins, ServiceNow, Cherwell, Remedy, and ACI.	This permission is recommended for those responsible for the integration between VM Essentials and integrated technologies.	
Admin: License Settings	None, Full	Allows or disallows access to the Licenses tab in Administration > Settings > Provisioning. When given to a Master Tenant user they may define specific subtenants in which the licenses may be used.	The Licenses tab is where software licenses may be added for tracking in VM Essentials. VM Essentials may then be configured to apply these licenses on provision. Currently, only Windows license types are available.	This permission is recommended for those responsible for managing Windows licenses.	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Admin: Log Settings	None, Full	Allows or disallows access to the Administration > Settings > Logs.	The Logs page is where logs are enabled. Syslog forwarding rules are also configured here.	This permission is recommended for those responsible for configuring VM Essentials log settings and integrations.	This permission is recommended to be set to None in the Tenant Role to restrict this access to Subtenant Users.
Admin: Message of the day	None, Full	Allows or disallows access to create and edit Message of the Day policies in Administration > Policies	The Policies page is where policies are defined. When creating a policy, users can select “Message of the Day” from the TYPE dropdown with this permission set to Full.	This permission is recommended for those responsible for publishing the Message of the Day.	This permission is recommended to be set to None in the Tenant Role to restrict this access from Subtenant Users.
Admin: Monitoring Settings	None, Full	Allows or disallows access to Administration > Settings > Monitoring	The monitoring settings page is where VM Essentials monitoring and monitoring integrations are configured. Monitoring checks can be turned on or off, and availability time frame, check interval period, and reported availability precision are also configured on this page.	This permission is recommended for those responsible for configuring VM Essentials monitoring settings and integrations.	This permission is recommended to be set to None in the Tenant Role to restrict this access from Subtenant Users.
Admin: Packages	None, Full	Allows or disallows access to the Packages tab on the Integrations page (Administration > Integrations)	The Plugins tab is where custom library packages (mpg) are added.	This permission is recommended for those responsible for managing the Library.	This permission is recommended to be set to None in the Tenant Role to restrict this access from Subtenant Users.
Admin: Plugins	None, Full	Allows or disallows access to the Plugins tab on the Integrations page (Administration > Integrations)	The Plugins tab is where custom plugins are added to extend VM Essentials functionality.	This permission is recommended for those responsible for extending VM Essentials functionality through custom plugins.	This permission is recommended to be set to None in the Tenant Role to restrict this access from Subtenant Users.
Admin: Policies	None, Read, Full	This setting determines the level of access to Administration > Policies. When given to a Master Tenant user the ability to define Global policies and associate them with one or many Subtenants is granted. When given to a Subtenant user, a global policy applies only to their subtenant.	The Policies page is where policies are defined. On create, the type of policy is selected, a name, description, and scope are defined.	This permission is recommended for those responsible for configuring and managing policies either at the Master Tenant or Subtenant.	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Admin: Profiles	none,read,full	Allows or disallows access to Profiles (Clouds)	Profiles are where Terraform, Key/Value profiles are created and managed.	This permission is recommended for those responsible for managing secrets and other metadata that needs to be accessed by provisioning and automation processes.	
Admin: Provisioning Settings	None, Full	Allows or disallows access to the Settings tab of the Administration > Settings > Provisioning page.	The Settings tab is where global provisioning settings are configured. For Master Tenant users, these include allowing Cloud selection, allowing host selection, requiring environment selection, showing pricing, hiding datastore stats on selection, cross-Tenant naming policies, and reusing naming sequence numbers. For both Master Tenant and Subtenant users, defining the deploy archive store, cloud-init setting, the PXE boot root password, and default App Blueprint types are available.	This permission is recommended to only be assigned to roles utilized within the Master Tenant.	
Admin: Roles	None, Read, Full	This setting determines access to the Administration > Roles page. When given to a Subtenant user, the ability to create user roles is granted. When given to a Master Tenant user, the ability to create and manage Tenant and Multi-Tenant Users roles is also granted.	The Roles page is where roles are defined. On create, a name and description are defined. Once created, the Role is accessed and feature access, Group access, Instance Type access and Blueprint access may be configured.	This permission is recommended for those responsible for configuring Role Based Access Control (RBAC) either globally or within their Subtenant.	
Admin: Service Plans	None, Read, Full	This setting determines access to Administration > Plans & Pricing. When given to a Subtenant user, access to the Plans tab is granted. When given to a user in the Master Tenant, the Price Sets and Prices tabs are also available.	The Plans tab is where service plans are defined. On create, a name and code (for API) are defined, display order, provisioning type, storage, memory, core count and the price may be configured. Additionally, the actions menu will allow group access to be scoped.	This permission is recommended for those responsible for defining and managing pricing and applying plans.	
Admin: Tenant	None, Read, Full	This setting determines access to the Administration > Tenants page. With this permission, local users may be created or deleted within each Tenant. Critical Note: Granting this permission to Subtenant users will expose all Tenants and Tenant users to the Subtenant.	The Tenant page is where all Tenants may be viewed, edited, created, or even deleted.	This permission is recommended to only be assigned to Roles utilized within the Master Tenant who are responsible for the creation, configuration, and/or deletion of Subtenants.	It is recommended this setting be set to None on the Tenant Role to restrict access for Subtenant users.

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Admin: Tenant - Impersonate Users	None, Full	This setting allows or disallows access to impersonate users. This selection is located on the Administration > Users page in the Actions menu. When set to Full, Impersonate selection is available.	This permission allows for users in the Master Tenant to impersonate users of the Master Tenant and Subtenants.	This permission is recommended to be assigned only to Roles utilized within the Master Tenant who are responsible for configuring RBAC or for supporting users.	It is recommended this setting be set to None on the Tenant Role to restrict access for Subtenant users.
Admin: Users	None, Read, Full	This setting determines access to the Administration > Users page (both Users and User Groups tabs). User Roles can also be set or edited when creating or editing a User on this page. Note: A Master Tenant user with the Admin: Tenants (Full) permission may also access and perform user management from the associated Tenant page.	The User tab is where all users may be viewed, edited, created, or even deleted. The User Groups tab is where User Groups may be viewed, edited, created, or even deleted. Within VM Essentials, a User Group may be selected during provisioning in order to add each group member's credentials to an Instance. When creating a User Group a name, description, server group (in Linux, name of the group to assign members), sudo access toggle, and a list of users are defined.	This permission is recommended for those responsible for managing users and RBAC.	
Admin: Whitelabel Settings	None, Full	Allows or disallows access to the Whitelabel tab in Administration > Settings.	The Whitelabel tab is where custom Tenant logos, colors, and security banners may be configured.	This permission is recommended for those responsible for branding tenants, whether they are Master Tenant users or individual Subtenant users.	

API Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
API: Billing	None, Read, Full	Allows or disallows access to invoices and projects via VM Essentials API/CLI.	The invoices API/CLI is used to generate bills and gather highly-granular costing data for supported Clouds. Read access allows list and get functions and Full allows access to post (refresh).	This permission is recommended for those responsible for generating invoices or projects.	It is recommended this setting be set to None on the Tenant Role to restrict access for Subtenant users.
API: Execution Request	None, Full	Allows or disallows access to an API endpoint.	This endpoint allows users to execute scripts on Instances, containers, or hosts and then polls for a response.	This permission is recommended for those responsible for arbitrary API script execution.	It is recommended this setting be set to None on the Tenant Role to restrict access for Subtenant users.

Backups Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Backups	None, View, Read, User, Full	Determines access to the Backups secton of VM Essentials UI, including the Summary, Jobs, Backups, and History subpages. The “User” permission allows access only to backup objects the user owns.	The Summary subpage allows the user to see the number of configured backups, the success rate, recent failures, and the size of the backups, as well as, the upcoming and in-progress backups. The Jobs subpage is where backup jobs may be created, cloned, edited or deleted. On create, a name, code (for use within the API), retention count, and schedule are selected (Note: Selectable schedules are defined Execution Schedules which are created in the Library > Automation). On the backups subpage, a list of configured backups is provided and new backups may be created or on-demand backups may be executed. On create, the place where the target exists is selected (Instance, Host, or Provider), the source is selected and a name is defined as well as the selected execution schedule. On the History subpage both the backups and restores tabs are available. Names, statuses, start times, durations and size may be viewed.	This permission is recommended for those responsible for performing the backup and restoration of workloads.	
Backups: Integrations	None, Read, Full	Determines access to the Backups > Integrations page.	From this page, backup integrations may be created, edited, or deleted. The page also provides the status of existing integrations. On create the integration product is selected and all associated connection and authentication information must be provided. Additionally, visibility is set to either public or private. Integrations available include Avamar, Commvault, Rubrik, Veeam, and Zerto.	This permission is recommended for those responsible for the integration between VM Essentials and backup technologies.	It is recommended this setting be set to None on the Tenant Role to restrict access for Subtenant users.

Catalog Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Catalog (Formerly Service Catalog: Catalog)	None, Full	Determines access to Provisioning > Catalog and Catalog in the Service Catalog Persona view	The Catalog page displays the complete list of Catalog Items that can be ordered from the Service Catalog	This permission is recommended for users who will order items from the Service Catalog	
Catalog: Dashboard (Formerly Service Catalog: Dashboard)	None, Read	Determines access to and Dashboard in Service Catalog Persona view	The Catalog Dashboard contains featured Catalog Items, recently-ordered Catalog items and Inventory items. The Catalog Dashboard is the default landing page for the Service Catalog Persona view	This permission is recommended for users who will use the Service Catalog	
Catalog: Inventory (Formerly Service Catalog: Inventory)	None, Full	Determines access to and Dashboard in Service Catalog Persona view	The Inventory is the complete list of user-owned items provisioned from the Service Catalog	This permission is recommended for users who will use the Service Catalog and need to be able to view details on the items they’ve provisioned from the Catalog	

Infrastructure Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Infrastructure: Boot	None, Read, Full	Determines access to the Integrations > Bootpage, including the Mapping, Boot Menus, Answer Files, Images, and Discovered MAC Addresses tabs.	VM Essentials includes a PXE Server to provide for rapid bare metal provisioning. The Boot page is where users may add, edit, or delete answer files, as well as, manage their own images or use existing ones. Boot menus and mappings are also managed here and discovered MAC addresses are displayed.	This permission is recommend for those responsible for bare metal provisioning.	
Infrastructure: Certificates	None, Read, Full	Determines access to the SSL Certificates tab on the Infrastructure > Keys& Certs page.	The SSL Certificates page is where certificates may be uploaded and managed. These certificates may then be used within VM Essentials when orchestrating load balancers.	This permission is recommended for personnel who will be orchestrating and provisioning load balancers.	
Infrastructure: Clouds	None, Read, Group, Full	Determines access to the Infrastructure > Clouds page. The “Group” permission limits the Cloud list page (Infrastructure > Clouds) to show only Clouds in their assigned Groups.	The Cloud page is where new Clouds are integrated with VM Essentials and existing Cloud integrations are managed. This includes creating a code for use within the API, the location, visibility, tenant, whether or not it should be enabled, and if VMs should be automatically powered on. Additionally, Clouds may be integrated from the Clouds tab of a Group detail page.	This permission is recommended for those responsible for configuring RBAC as well as those responsible for VM Essentials Cloud Integrations.	
Infrastructure: Clusters	None, Read, Group, Full	Determines access to the Infrastructure > Clusters page.	The Clusters page allows you to create and manage Kubernetes, Docker, and KVM Clusters, as well as Cloud-specific Kubernetes services such as EKS.	This permission is recommend for those creating and managing containers or container services.	
Infrastructure: Compute	None, Read, Full	Determines access to the Infrastructure > Hostspage, including the Hosts, Virtual Machines, and Bare Metal tabs.	The Hosts page provides for viewing and managing hosts, virtual machines, and bare metal hosts. On the bare metal hosts page, hosts may come from PXE boot or may be manually added. On the Hosts page hypervisors and Docker hosts are displayed. The Virtual Machines page lists all VMs. On all three pages actions may be performed against machines. Additionally, views may be refined by altering the columns displayed and CSV/JSON exporting of lists is available.	This permission is recommend for those whom need to take action on machines and those responsible for bare metal provisioning.	
Infrastructure: Credentials	None, Read, Full	Determines access to the Credentials tab in Infrastructure > Trust	The credentials tab allows you to create and manage credential sets stored internally and in external Cypher server integrations	This permission is recommended for those responsible for maintaining credentials	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Infrastructure: Groups	None, Read, Full	Determines access to the Infrastructure > Groups page.	The Groups page is where VM Essentials Groups are created and given a code for use within the API. Additionally, the DNS service, CMDB, service registry, and config management may be selected. Existing Clouds/Hosts or new Clouds/Hosts are added to the Group and virtual or bare metal machines may be viewed.	This permission is recommended for those responsible for configuring Role Based Access Control (RBAC).	
Infrastructure: Keypairs	None, Read, Full	Determines access to the Key Pairs tab on the Infrastructure > Keys& Certs page.	The Keypairs page allows for ease in accessing instances via SSH. On create a name, public key, private key, and passphrase are entered.	This permission is recommended for those whom utilize VM Essentials deployment and management of Linux Instances.	
Infrastructure: Kubernetes Control	None, Full	Determines access to the Control tab on Kubernetes Cluster detail pages (Infrastructure > Clusters > Selected Kubernetes Cluster > ControlTab)	Run `kubectl` commands, apply templates, and run workloads on the Kubernetes Cluster	This permission is recommended for Kubernetes Cluster administrators	
Infrastructure: Load Balancers	None, Read, Full	Determines access to the Infrastructure > Load Balancers page, including both the Load Balancers and Virtual Servers tabs.	The Load Balancers page is where new load balancer integrations may be configured. Additionally, existing integrations may be managed. The Virtual Servers page is where virtual servers are managed to include policies, pools, profiles, monitors, nodes, and rule scripts may be managed.	This permission is recommended for those responsible for integrating VM Essentials with load balancers as well as those responsible for managing virtual servers.	
Infrastructure: Move Servers	None, Full	Determines access to the “Change Cloud” action on server detail pages (Infrastructure > Compute > Virtual Machines tab > SelectedVM > Actions > Change Cloud)	Change Cloud allows server records to be migrated from one Cloud to another. Note that this is not a migration tool but simply allows for upkeep of records in VM Essentials.	This permission is recommended for appliance administrators. See other sections of VM Essentials documentation for more information on the use of this feature.	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Infrastructure: Networks	None, Read, Group, Full	Determines access to the Infrastructure > Networks page, including the Networks, network groups, and integrations tabs. The "Group" permission setting allows access to objects shared to Groups associated with the user.	The Networks page is where networks are configured for DHCP or static IP assignment and existing networks are displayed. The Network Groups page is where networks are grouped to allow round robin provisioning among the group. The Integrations page is where IPAM, DNS, security, service registry, and virtual network tools are integrated. These include Cisco ACI, VMware NSX T and V, Infoblox, Bluecat, phpIPAM, SolarWinds, Stealth, Microsoft DNS, PowerDNS, and Route 53.	This permission is recommended for those responsible for integration with network technologies and the configuration and management of networks to be used during provisioning.	
Infrastructure: Policies	None, Read, Full	Determines access to the Policies tabs on the Group and Cloud detail pages (Infrastructure > Groups > selected Group OR Infrastructure > Cloud > selected Cloud).	Policies can be created from this tab which are scoped to the Cloud or Group being viewed.	This permission is recommended for users who will need to set quotas which pertain specifically to Groups or Clouds the user has access to.	
Infrastructure: Security Groups	None, Read, Full	Determines access to the Security Groups tab on the Infrastructure > Networks page.	The Security Groups page is where Security Groups (aka virtual firewalls) are defined.	This permission is recommended for those responsible for firewall configuration and management.	
Infrastructure: State	None, Read, Full	Determines access to the power state toggle on the Infrastructure > Hostspage.	This toggle moves Hosts between a started and stopped state.	This permission is recommended for those responsible for managing Hosts.	
Infrastructure: Storage	None, Read, Full	Determines access to the Infrastructure > Storage page, including the Buckets, File Shares, Volumes, Data Stores, and Servers tabs.	The Servers page is where storage integrations are configured. Integrations available include 3Par, AWS S3, Dell EMC ECS and Isilon, Huawei or Open Telekom OBS and Huawei, Open Telekom, OpenStack SFS. The Volumes page is where storage volumes may be created or viewed. The File Shares page is where File Shares of types CIFS, Dell EMC ECS or Isilon, local storage, and NFSv3 may be configured. The Buckets page is where storage buckets of type AWS S3, Alibaba, Azure, Open Telekom OBS, OpenStack Swift, Racspace CDN may be created. Storage buckets are used for Backup, Archives, and Virtual Images. The Data Store page is where permissions to data stores may be managed and new data stores are added.	This permission is recommended for those responsible for storage integrations and configurations.	This permission is recommended to be set to None on the Tenant Role to restrict access to Subtentant users.

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Infrastructure: Storage Browser	None, Read, Full	Determines file browsing access to buckets and file shares on the Buckets and File Shares tabs of the Infrastructure > Storage page.	The Storage Browser permission allows users who also have appropriate Infrastructure: Storage permission to browse, add files and folders, download, and delete from the buckets and file shares.	This permission is recommended for those who need to browse storage.	
Infrastructure: Trust Integrations	None, Read, Full	Determines access to the Integrations tab of the Infrastructure > Keys& Certs page.	The Integrations tab is where new trust integrations can be configured.	This permission is recommended for those responsible for the integration between VM Essentials and trust providers.	This permission is recommended to be set to None on the Tenant Role to restrict access to Subtentant users.

Library Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Library: App Blueprints (Formerly Provisioning: Blueprints)	None, Read, Full	Determines access to the Library > Blueprints > App Blueprints page.	The Blueprints page allows for the creation of pre-configured, multi-tier application definitions which can be deployed via the Apps page. With this permission the blueprint type of VM Essentials is available.	This permission is recommended for those responsible for defining VM Essentials-type Blueprints.	
Library: Blueprints - ARM (Formerly Provisioning: Blueprints - ARM)	None, Provision, Full	Determines access to ARM-type Blueprints on the Library > Blueprints > App Blueprints page. The “Provision” permission allows for provisioning Apps from ARM Blueprints without the ability to create or edit them.	The Blueprints page allows for the creation of pre-configured, multi-tier application definitions which can be deployed via the Apps page. With this permission the blueprint type of ARM is available.	This permission is recommended for those responsible for defining ARM blueprints.	
Library: Blueprints - CloudFormation (Formerly Provisioning: Blueprints - CloudFormation)	None, Provision, Full	Determines access to CloudFormation-type Blueprints on the Library > Blueprints > App Blueprints page. The “Provision” permission allows for provisioning Apps from CloudFormation Blueprints without the ability to create or edit them.	The Blueprints page allows for the creation of pre-configured, multi-tier application definitions which can be deployed via the Apps page. With this permission the blueprint type of CloudFormation is available.	This permission is recommended for those responsible for defining CloudFormation blueprints.	
Library: Blueprints - Helm (Formerly Provisioning: Blueprints - Helm)	None, Provision, Full	Determines access to Helm-type Blueprints on the Library > Blueprints > App Blueprints page. The “Provision” permission allows for provisioning Apps from Helm Blueprints without the ability to create or edit them.	The Blueprints page allows for the creation of pre-configured, multi-tier application definitions which can be deployed via the Apps page. With this permission the blueprint type of Helm is available.	This permission is recommended for those responsible for defining Helm blueprints.	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Library: Blueprints - Kubernetes (Formerly Provisioning: Blueprints - Kubernetes)	None, Provision, Full	Determines access to Kubernetes-type Blueprints on the Library > Blueprints > App Blueprints page. The “Provision” permission allows for provisioning Apps from Kubernetes Blueprints without the ability to create or edit them.	The Blueprints page allows for the creation of pre-configured, multi-tier application definitions which can be deployed via the Apps page. With this permission the blueprint type of Kubernetes is available.	This permission is recommended for those responsible for defining Kubernetes blueprints.	
Library: Blueprint - Terraform (Formerly Provisioning: Blueprints - Terraform)	None, Provision, Full	Determines access to Terraform-type Blueprints on the Library > Blueprints > App Blueprints page. The “Provision” permission allows for provisioning Apps from Terraform Blueprints without the ability to create or edit them.	The Blueprints page allows for the creation of pre-configured, multi-tier application definitions which can be deployed via the Apps page. With this permission the blueprint type of Terraform is available.	This permission is recommended for those responsible for defining Terraform blueprints.	
Library: Catalog Items (Formerly Tools: Self Service)	None, Read, Full	Determines access to Library > Blueprints > Catalog Items	Library > Blueprints > Catalog Items allows administrators to configure Catalog Items for the Library Catalog and Self Service Persona users	This permission is recommended for those responsible for creating and managing Library Catalog Items.	
Library: Instance Types (Formerly Provisioning: Library)	None, Read, Full	Determines access to the Library > Blueprints > Instance Types	Library > Blueprints > Instance Types is where Instance Types are created and maintained.	This permission is recommended for those responsible for managing the Instance Types.	
Library: Integrations (Formerly Provisioning: Automation Integrations)	None, Read, Full	Determines access to Library > Integrations.	Library > Integrationsis where Library Automation created and maintained.. These include Chef, Puppet, Ansible, Ansible Tower and vRealize Orchestrator.	This permission is recommended for those responsible for the integration between VM Essentials and integrated automation technologies.	
Library: Packages	None, Read, Full	Determines access to Library > Templates > Cluster Packages.	Library > Templates > Cluster Packages is where Cluster Packages are created or edited. Cluster Packages are associated with Cluster Layouts	This permission is recommended for those responsible for Cluster Layout templating	
Library: Options	None, Read, Full	Determines access to Library > Options - Inputs (Option Types) and Option Lists.		This permission is recommended for those responsible for creating and managing Library Inputs (Option Types) and Option Lists.	
Library: Scheduling - Execute (Formerly Provisioning: Scheduling - Execute)	None, Read, Full	Determines access to Library > Automation > Execute Scheduling.	The Execute Scheduling is where time schedules for Jobs, including Task, Workflow, and Backup Jobs are created and managed.	This permission is recommended for those responsible to create and manage schedules to be selected when scheduling jobs.	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Library: Scheduling - Power (Formerly Provisioning: Scheduling - Power)	None, Read, Full	Determines access to Library > Automation > Power Scheduling.	Power Scheduling is where startup and shutdown times are created, these schedules can be applied via policy or manaully.	This permission is recommended for those responsible to create and manage power schedules.	
Library: Tasks (Formerly Provisioning: Tasks)	None, Read, Full	Determines access to Library > Automation > Tasks and Library > Automation > Workflows.	Library > Automation > Tasks is where Tasks are created and managed. Library > Automation > Workflows is where Workflows are created and managed. Workflows are used to execute one or many tasks during specified phases.	This permission is recommended for those responsible for creating provisioning and operational scripts.	
Library: Tasks - Script Engines (Formerly Provisioning: Tasks - Script Engines)	None, Full	Determines access to **Execute Target** of **Local** for Tasks.	This permission limits Tasks from being able to run on the Morpheus appliance(s). Additionally, Task Types that only contain the **Execute Target** of **Local** will be removed, such as: Groovy, Javascript, and Python Task Types.	This permission is recommended for those responsible for Tasks that may need to execute on the appliance(s).	
Library: Templates	None, Read, Full	Determines access to Library > Templates	Library > Templates is where Spec Templates, File Templates, Script Templates and Security Packages are created and managed.	This permission is recommended for those responsible for creating and managing Spec Templates, File Templates, Script Templates and Security Packages.	
Library: Thresholds (Formerly Provisioning: Thresholds)	None, Read, Full	Determines access to Library > Automation > Scale Thresholds.	Scale Thresholds is where preconfigured settings for auto-scaling Instances are configured. When adding auto-scaling to an Instance, existing Scale Thresholds can be selected to define auto-scaling rules.	This permission is recommended for those responsible for defining auto-scaling for Instances.	This permission is recommended to be set to None or Read on the Tenant Role to restrict access for Subtenant users.
Library: Virtual Images (Formerly Provisioning: Virtual Images)	None, Read, Full	Determines access to the Library > Virtual Images page.	Library > Virtual Images is where user and system Virtual Images are managed.	This permission is recommended for those who are responsible for image management.	

Lifecycle Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Environment Variables	None, User, Read, Full	Allows access to the Environments tab of the Instance detail page	Allows Instance environment variables to be edited. If set to “User” level only environment variables of Instances owned by the currently logged in user may be edited.	This permission is recommended for those needing management control over Instances	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Lifecycle: Extend Expirations	None, User, Full	Determines if the user can extend an expiration or shutdown Policy	Allows the user to extend automated shutdown or expiration policies set against any workload (“full” permission) or against the user’s own workloads (“user” permission)	This permission is recommended for administrators or those who need to be able to extend Policies set against their own workloads (“user” level permission)	
Power Control	None, User, Full	Allows access to power state controls for Instances and servers, including stopping, starting, restarting and suspending.	Allows the user to change the current power state of Instances and servers	This permission is recommended for those needing management control over Instances	
Reconfigure	None, User, Full	Allows general access to Instance and server reconfigure (resize) feature. See additional reconfigure permissions below for more granular control over specific reconfigure functionality.	Allows general access to reconfigure features for Instances and servers. “User” level permission allows only Instances and servers owned by the currently logged in user to be reconfigured.	This permission is recommended for those needing management control over Instances	
Reconfigure: Change Plan	None, User, Full	Allows the user to change the Instance service plan	When reconfiguring, the user may change the service plan associated with the Instance. “User” level permission allows only Instances owned by the currently logged in user to have their plans changed.	This permission is recommended for those needing management control over Instances	
Reconfigure: Disk Add	None, User, Full	Allows the user to add disks to an Instance or server during reconfigure.	When reconfiguring, the user may add disks to the selected Instance or server. “User” level permission allows only Instances owned by the currently logged in user to have their disks changed.	This permission is recommended for those needing management control over Instances	
Reconfigure: Disk Change Type	None, User, Full	Allows the user to change the datastore or volume type during reconfigure.	When reconfiguring, the user may update datastore or volume types. “User” level permission allows only Instances owned by the currently logged in user to have their disk types changed.	This permission is recommended for those needing management control over Instances	
Reconfigure: Disk Modify	None, User, Full	Allows the user to modify an attached disk during reconfigure.	When reconfiguring, the user may modify disks attached to the Instance. “User” level permission allows only Instances owned by the currently logged in user to have their disks changed.	This permission is recommended for those needing management control over Instances	
Reconfigure: Disk Remove	None, User, Full	Allows the user to remove disks or volumes during reconfigure.	When reconfiguring, the user may remove disks attached to the Instance or server. “User” level permission allows only Instances owned by the currently logged in user to have their disks removed.	This permission is recommended for those needing management control over Instances	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Reconfigure: Network Add	None, User, Full	Allows the user to add a network adapter during reconfigure.	When reconfiguring, the user may add a network interface to the Instance or server. “User” level permission allows only Instances owned by the currently logged in user to have network interfaces added.	This permission is recommended for those needing management control over Instances	
Reconfigure: Network Modify	None, User, Full	Allows the user to edit network adapters during reconfigure.	When reconfiguring, the user may edit network interfaces on the Instance or server. “User” level permission allows only Instances owned by the currently logged in user to have network interfaces modified.	This permission is recommended for those needing management control over Instances	
Reconfigure: Network Remove	None, User, Full	Allows the user to remove network adapters during reconfigure.	When reconfiguring, the user may remove network interfaces on the Instance or server. “User” level permission allows only Instances owned by the currently logged in user to have network interfaces removed.	This permission is recommended for those needing management control over Instances	
Lifecycle: Retry/Cancel	None, Full	Determines access to retry and cancel buttons for Tasks (for example, in the History tab of an Instance detail page)	Retry and cancel functionality allows failed automation Tasks to be retried or stuck Tasks to be stopped from various places within VM Essentials UI (such as in the History tab of an Instance detail page)		

Monitoring Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Monitoring	None, Read, User, Full	Determines level of access to the Monitoring section of VM Essentials UI, including the Status, Apps, Checks, Groups, Incidents, Contacts, and Alert Rules subpages. The “User” permission will allow access only to objects the user owns.	The Checks page is where automatically-created checks are customized or new checks are created. The Groups and Apps pages are where checks may be grouped. The Incidents page is where incidents are created upon Check failure. The Contacts page is where contacts may be added for notifications. The Alert Rules page is where notification are configured.	This permission is recommended for those responsible for monitoring applications, incidents, or configuring notifications.	
Monitoring: Logs (Formerly Logs)	None, Read, User, Full	Determines level of access to the Logs section of VM Essentials UI. The “User” permission will allow access only to objects the user owns.	Monitoring > Logs is where Instance and Server logs may be viewed (also must be enabled in order to view Appliance logs from Administration > Health > Morpheus Logs Logs when health permission is also enabled).	This permission is recommended for those who should have access to Instance and Server logs.	Setting permission to Full on the Tenant Role will give Subtenant users full access to all logs appliance-wide, including to workloads living in other Tenants, for any Subtenant users who also have Full permission on their User Role. It’s recommended that you set this permission to User on the Tenant Role so that Subtenant users are not able to see logs for workloads other than their own.

Networks Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Networks: DHCP Relays	None, Read, Full	Determines access to the DHCP Relays in applicable network integrations	Allows DHCP Relays to be viewed, created and managed	This permission is recommended for those tasked with network management	
Networks: DHCP Servers	None, Read, Full	Determines access to the DHCP Servers in applicable network integrations	Allows DHCP Servers to be viewed, created and managed	This permission is recommended for those tasked with network management	
Networks: Domains	None, Read, Group, Full	Determines access to the Domains tab on the Infrastructure > Network page. Domains may be scoped for specific Group access. If the Group-level permission is selected here, users will only have visibility into Domains scoped to Groups they can access.	The Domains page is where network domains are managed. Domains are used for setting FQDNs, joining Windows Instances to domains, and creating A-Records with DNS integrations. On create the domain controller and credentials for domain join must be provided.	This permission is recommended for those responsible for VM Essentials DNS and domain-join integrations.	
Networks: Firewalls	None, Read, Manage Rules, Full	Determines access to the Firewall tab on applicable network integrations detail pages. When the “Manage Rules” permission is given, users have read-only access to firewall groups and the ability to create and manage firewall rules on those groups	The Firewall tab is where network firewall groups and rules are viewed, created and managed	This permission is recommended for those tasked with network security management	
Networks: Floating IPs	None, Read, Full	Determines access to the Floating IPs tab on the Network list page (Infrastructure > Network)	The Floating IPs tab is where Floating IPs from supported Clouds are listed once synced into VM Essentials Users may also release unattached Floating IPs from this page and link through to any workloads which have Floating IPs attached	This permission is recommended for those tasked with network management	
Networks: IP Pools	None, Read, Group, Full	Determines access to the IP Pools tab on the Network list page (Infrastructure > Network). IP Pools may be scoped for specific Group access. If the Group-level permission is selected here, users will only have visibility into IP Pools scoped to Groups they can access.	The IP Pools tab is where IP pools from various networks are displayed. Detail pages for IP pools can also be accessed here	This permission is recommended for those tasked with IP address management	
Networks: Integration	None, Read, Full	Determines access to the Integrations tab on the Network list page (Infrastructure > Network)	The integrations tab is where network integrations can be viewed, added and managed. Additionally, the detail pages for network integrations are accessed here	This permission is recommended for those tasked with handling network integrations and their use within VM Essentials	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Networks: Proxies	None, Read, Full	Determines access to the Proxies tab on the Infrastructure > Networks page.	The Infrastructure Networks Proxies page is where Proxy configurations are stored, which are available for use by the provisioning engines.	This permission is recommended for those responsible for configuring proxies to be used when provisioning.	
Networks: Router Firewalls	None, Read, Full	Determines access to Firewall tabs on Router Detail pages (Infrastructure > Network > Routers tab > SelectedRouter)	The Firewall tab is where firewall rules are viewed, created, and managed	This permission is recommended for those responsible for managing firewall rules	
Networks: Router Interfaces	None, Read, Full	Determines access to Interfaces tabs on Router Detail pages (Infrastructure > Network > Routers tab > SelectedRouter)	The Interface tab is where router interfaces can be viewed, created and managed	This permission is recommended for those responsible for network traffic flow	
Networks: Router NAT	None, Read, Full	Determines access to the NAT tab on Router Detail pages (Infrastructure > Network > Routers tab > SelectedRouter)	The NAT tab is where NAT rules are viewed, created, and managed	This permission is recommended for those responsible for network traffic flow	
Networks: Router Redistribution	None, Read, Full	Determines access to Route Redistribution tabs on Router Detail pages (Infrastructure > Network > Routers tab > SelectedRouter)	The Route Redistribution tab is where redistribution rules are viewed, created, and managed	This permission is recommended for those responsible for redistribution rules	
Networks: Router Routes	None, Read, Full	Determines access to Routing tabs on Router Detail pages (Infrastructure > Network > Routers tab > SelectedRouter)	The Routing tab is where routes are viewed, created, and managed	This permission is recommended for those responsible for network route management	
Networks: Routers	None, Read, Group, Full	Determines access to the Routers tab on the Infrastructure > Networks page. The “Group” permission setting allows access to objects shared to Groups associated with the user.	The Routers page is where virtual routers are created and managed from Cloud and Network integrations.	This permission is recommended for those responsible for network management.	
Networks: Server Groups	None, Read, Full	Determines access to			
Networks: Static Routes	None, Read, Full	Determines access to the routing tab on a router detail page (/infrastructure/networks/routes)	The routers tab is where routes are created and managed	This permission is recommended for those responsible for network management	

Operations Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Operations: Activity	None, Read	Determines access to the Activity and History tabs on the Operations > Activity page.	The Activity page displays four types of recent activities: Provisioning, Alerts, Backups, and Permissions.	This permission is recommended for those responsible to monitor or view activities and their statuses within VM Essentials.	
Operations: Alarms	None, Read, Full	Determines access to the Alarms tab in the Activity section (Operations > Health)	The Alarms tab is where alarms are listed and acknowledgement actions can be taken against them	This permission is recommended for those responsible for monitoring	
Operations: Analytics	None, Read, Full	Determines access to the Operations > Analytics page.	The Analytics page gives administrators the ability to break down costs and usage, then filter the results by relevant delineations including Groups, Clouds, Tenants or even tag values.	This permission is recommended for those responsible for understanding utilization and costs.	
Operations: Approvals	None, Read, Full	Determines access to the Operations > Approvals page.	When a Provision Approval-type Policy is enabled for a Group or Cloud, an approval request will be created on each relevant provision attempt. These approvals can be handled directly in VM Essentials or dealt with in ServiceNow with a properly-configured integration.	This permission is recommended for those responsible for approving, denying, or canceling approval requests.	
Operations: Budgets	None, Read, Full	Determines access to the Operations > Budgetspage.	The Budgets page is where budgets are created and applied to clouds, tenants, users, or groups.	This permission is recommended for those responsible for managing budgets.	
Operations: Dashboard	None, Read	Determines access to the Operations > Dashboard page (default VM Essentials landing page).	The Dashboard page is a single pane of glass showing quick, easy-to-read performance and configuration information about the VM Essentials environment.	“Read” permission is recommended for all users. When set to None, Operations > Reports becomes the default landing page and attempts to go to the Dashboard will redirect users to their User Settings page.	
Operations: Guidance	None, Read, Full	Determines access to the Operations > Guidance page.	The Guidance page shows recommendations for resource and cost-utilization optimization.	This permission is recommended for those responsible to optimize utilization and costs of Cloud-based resources.	
Operations: Invoices	None, Read, Full	Determines access to the Invoices tab in Operations > Costing	The Invoices tab allows access to highly-granular historical costing data	This permission is recommended for those responsible for generating invoices and analyzing spend	
Operations: Reports	None, Read, Full	Determines access to the Operations > Reports page.	The Reports page is where reports may be generated and exported into JSON or CSV format.	This permission is recommended for those responsible for account, infrastructure, provisioning, usage, and cost reports.	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Operations: Usage	None, Read, Full	Determines access to the Usage tab on the Operations > Activity page.	The Usage tab shows billing information for Instances and hosts that have pricing configured on their Service Plans.	This permissions is recommended for those responsible for cost accounting.	
Operations: Wiki	None, Read, Full	Determines access to the Operations > Wiki page.	The Wiki page allows easy UI, API and CLI access to information to be referenced or shared with others. Wiki pages encompass individual Clouds, Groups, Servers, Instances, Clusters, and other pages can be manually created. Wiki pages from resources are accessible from the Operations > Wiki page or within individual resource detail pages on their respective Wiki tabs.	This permission is recommend for those responsible for documentation and knowledge management.	

Projects Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Projects	None, Read, Full	Determines access to Projects through VM Essentials API	Projects are used to associate resources together and apply common tags to their invoices	This permission is recommended for those responsible for cost analysis and invoice reporting	

Provisioning Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Provisioning: Administrator	None, Full	When editing an Instance (Provisioning > Instances > selected Instance > EDITbutton), this permission determines access to changing the owner of an Instance.	Allows you to change the owning user of an Instance.	This permission is recommended for those responsible to ensure all instances are owned by appropriate personnel.	
Provisioning: Advanced Node Type Options	None, Full	This allows or disallows access to the “Extra Options” field of the Node Types tab on the Library page when the Node Type Technology value is set to “VMware”.	When VMware technology type is selected for a new or existing Node Type (Library > Blueprints > Node Types), the “Extra Options” field will be available in the VMware VM Options section. These allow defining advanced vmx-file parameters during provisioning.	This permission is recommended for those responsible for managing VMware Node Types (images).	
Provisioning: Apps	None, Read, User, Full	Determines access to the Provisioning > Apps page. The “User” permission will allow access to only object the user owns.	The Apps page allows Instances to be grouped and tiered logically into Apps. From this page, Apps can be deployed from existing Blueprints and Instances can be added to existing Apps. Security groups and environmental variables (Linux Only) may be added and edited. The App log, history, and monitoring tabs may be viewed.	This permission is recommended for those responsible for provisioning.	
Provisioning: Code Deployments	None, Read, Full	Determines access to the Deployments tab on the Provisioning > Code page.	The Deployments page provides the ability to use git, fetch from a url, or upload a file to be utilized during the provisioning of an Instance or pushed to an existing Instance.	This permission is recommended for those responsible for providing and managing software.	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Provisioning: Code Integrations	None, Read, Full	Determines access to the Integrations tab on the Provisioning > Code page.	From this page code integrations may be created, edited, or deleted. Integrations available include Git, Github, and Jenkins.	This permission is recommended for those responsible for the integration between VM Essentials and code repositories and services.	
Provisioning: Code Repositories	None, List Files, Read, Full	Determines access to the Deployments tab on the Provisioning > Code page.	The Code Repositories contains the repositories integrated with VM Essentials allowing users to browse repositories folders and files and view file contents from any branch, trigger a refresh, and create tasks, scripts and templates directly from the repos.	This permission is recommended for those responsible for providing and managing software.	
Provisioning: Execute Script	None, Full	Determines access to the Run Script and Apply Template selections from the Actions menu on an Instance detail page	These selections bring up a menu allowing the user to select a script and run it against the viewed Instance or select a template to write to the Instance	This permission is recommended for those running day two automations against existing Instances	
Provisioning: Execute Task	None, Full	Determines access to the Run Task selection from the Actions menu on an Instance detail page	This selection brings up a menu allowing the user to select a Task and run it against the viewed Instance	This permission is recommended for those running day two automations against existing Instances	
Provisioning: Execute Workflow	None, Full	Determines access to the Run Workflow selection from the Actions menu on an Instance detail page	This selection brings up a menu allowing the user to select a Workflow and run it against the viewed Instance	This permission is recommended for those running day two automations against existing Instances	
Provisioning: Executions	None, Read, User	Determines access Provisioning > Executions. When the permission level is set to “User” only the executions owned by the current user are shown	Provisioning > Executions is where Task, Workflow, and Security Scan execution output can be viewed	This permission is recommended for those who are responsible for managing or troubleshooting Task, Workflow, and Security Scan executions.	
Provisioning: Import Image	None, Full	Determines access to the Import as Image and Clone to Image selections from the Actions menu on an Instance detail page	These selections allow users to create an image from an existing Instance or import the Instance as an image to a selected bucket	This permission is recommended for those responsible for managing the library of provisionable items	
Provisioning: Instances: Add	None, Full	Gives access to create Instances. Without this permission the user cannot directly add Instances.	The “+ ADD” button will not be visible on the Instances List Page if permission is set to “None” and the user will not have access to Instance create API actions as well	This permission is recommended for any user who needs to be able to provision Instances	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Provisioning: Instances: Clone	None, User, Full	Determines the presence of the “Clone” selection under the Actions menu on the Instance detail page and Instance clone API functionality	The “Clone” selection will not be available under the “Actions” menu on the Instance detail page if permission is set to “None” and the user will not have access to similar API actions. If permission is set to “User”, only Instances owned by the currently logged in user may be cloned.	This permission is recommended for any user who needs to be able to manage Instances	
Provisioning: Instances: Delete	None, User, Full	Determines the presence of the “Delete” button on the Instance detail page, delete bulk action on the Instances list page, and Instance delete API functionality	The “Delete” button will not be available on the Instance detail page and the delete action will not be available from the Instances list page if permission is set to “None” and the user will not have access to similar API actions. If permission is set to “User”, only Instances owned by the currently logged in user may be deleted.	This permission is recommended for any user who needs to be able to manage Instances	
Provisioning: Instances: Edit	None, User, Full	Gives access to the Edit Instances modal for existing Instances (and corresponding API functionality). This allows the user to edit an Instance display name, tags, or Input (custom option) values	The “EDIT” button will not be visible on the Instances List Page if permission is set to “None” and the user will not have access to Instance edit API actions. If permission is set to “User”, only Instances owned by the currently logged in user may be edited.	This permission is recommended for any user who needs to be able to manage Instances	
Provisioning: Instances: Force Delete	None, Full	Determines access to the force delete option when deleting Instances	The force delete option (checkbox) will not be available when deleting Instances if this permission is not given. Force deleting allows VM Essentials to delete an Instance object even when it is unable to confirm the delete happened in the target cloud. Occasionally, this may be necessary but improper use can cause orphaned objects.	This permission is recommended for any user who needs to be able to manage Instances	
Provisioning: Instances: List	None, User, Full	Controls which Instances are listed on the Instances list page (Provisioning > Instances). When set to “User”, only Instances owned by the currently logged in user will be displayed.		This permission is recommended for any user who needs to be able to manage Instances	
Provisioning: Instances: Lock/Unlock	None, User, Full	Gives access to the lock/unlock actions on Instance detail pages (and corresponding API functionality). This allows the user to lock or unlock Instances which reduces the chances of accidental removal of important workloads.	The Lock/Unlock selections will not be visible in the Actions menu on the Instances List Page if permission is set to “None”. If permission is set to “User”, only Instances owned by the currently logged in user may be locked or unlocked.	This permission is recommended for any user who needs to be able to manage Instances	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Provisioning: Instances: Remove From Control	None, User, Full	Gives access to deleting an Instance in VM Essentials only. The instance remains in the target cloud. This may only be done for brownfield workloads which were converted to managed VM Essentials Instances		This permission is recommended for any user who needs to be able to manage Instances	
Provisioning: Instances: Scale	None, User, Full	Gives access to the scale tab on Instance detail pages which allow configuration of automated scaling thresholds (and corresponding API functionality). This allows the user to control scaling thresholds and add/remove nodes from an Instance.	The Scale tab on the Instance detail pages will not be visible and the user will not be able to add/remove nodes from Instances if the permission is set to “None”. If permission is set to “User”, only Instances owned by the currently logged in user may be scaled.	This permission is recommended for any user who needs to be able to manage Instances	
Provisioning: Instances: Settings	None, User, Read, Full	Gives access to configuration changes if the Instance supports dynamic settings templates			
Provisioning: Job Executions	None, Read	Determines access to the Job Executions tab on the Provisioning > Jobs page.	The Job Executions page contains execution history of completed jobs, including any process outputs and error messages.	This permission is recommended for those who are responsible for managing or troubleshooting jobs.	
Provisioning: Jobs	None, Read, Full	Determines access to the Jobs tab on the Provisioning > Jobs page.	The Jobs page is where jobs are scheduled for the execution of automation Tasks and Workflows against Instances or servers.	This permission is recommended for those responsible to schedule the exectution of Tasks or Workflows.	
Provisioning: Remote Console	None, User, Full	Determines access to the console on a Host detail page (Infrastructure > Hosts > selected Host, VM, or Bare Metal resource > Consoletab). The “User” permission gives access to the console only for resources the logged in user owns.	Remote console access for Instances, hosts, virtual machines, and bare metal.	This permission is recommended for those who need console access for provisioned Cloud resources.	
Provisioning: Remote Console Auto Login	No, Yes	This allows or disallows the ability to automatically log into the remote console.	VM Essentials will automatically log into the machine using the credentials defined on the VM or Host. The credentials are defined either from the virtual image used, added via cloud-init or VMware Tools using the global cloud-init settings (Administration > Settings > Provisioning), or the Linux or Windows settings defined in User Settings.	This permission is recommended when an organization utilizes VM Essentials to create user accounts on provisioned or managed machines, as well as, allow remote console access.	

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Provisioning: Service Mesh	None, Read, User, Full	Determines access to the Provisioning > ServiceMesh page, including the Services and DNS tabs. The “User” permission will allow access only to objects the user owns.	The Service Mesh page displays container services and DNS information. A service mesh ensures fast and reliable communication between containerized application services.	This permission is recommended for those responsible for container management.	
Provisioning: State	None, Read, Full	Determines access to the State tab for a Terraform Instance or App	The State tab is where **Terraform state management** is handled for Terraform Instances or Apps	This permission is recommended for those responsible for any Terraform-based workloads	

Security Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Security: Scanning	None, Read, Full	Determines access to the Security Packages tab on the Jobs list page (Provisioning > Jobs), Security Scanning type Jobs, and Security Subtab inside the Software tab on a server detail page where the results of security scans are viewed	Allows access to view, create, and run security scans on existing systems, as well as view the results of previously-run scans	This permission is recommended for those responsible for security compliance of existing systems	

Snapshots Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Snapshots	None, Read, Full	Determines access to the “Create Snapshot” function in the Actions menu on an Instance detail page (Provisioning > Instances > selected Instance).	If utilizing a VMware Cloud, the ability to create snapshots is available on the Instance detail page (Provisioning > Instances > selected Instance).	This permission is recommended for Instance owners who should be allowed to take snapshots.	
Snapshots: Linked Clone	None, Full	For VMware Cloud Instances, this controls access to the ability to create linked clone snapshots on the Instance detail page			

Tools Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Tools: Archives	None, Read, Full	Determines access to the Tools > Archives page.	Archives provides a way to store files and make them available for download by scripts and users. Archives are organized by buckets. Each bucket has a unique name that is used to identify it in URLs and Scripts.	This permission is recommended for those responsible for storage or scripts which will use the Archive.	
Tools: Cypher	None, Read, User, Full, Full Decrypt	Determines access to the Tools > Cypher page. The “User” permission will allow access only to objects the user owns. The “Full Decrypt” permission will allow for decryption of secrets.	Secure key/value store. Cypher keys can be used in scripts.	Recommended for those who need to store or use security key value pairs.	
Tools: Image Builder	None, Read, Full	Determines access to the Tools > Image Builder page, Image Builds, Boot Scripts, and Preseed Scripts tabs.	The VM Essentials Image Builder tool creates vmdk, qcow2, vhd and raw images. The Image Builder creates a blank VM in VMware, attaches an OS ISO, executes a boot script on the VM at startup via VNC, which calls a preseed script that runs the unattended OS installation and configuration. VM Essentials then executes an OVA export of the completed vmdk to the target storage provider and converts the image to all other specified formats.	Recommended for those who are responsible for image creation.	
Tools: Kubernetes	None, Read, User, Full	Allows for the management of Kubernetes clusters via the API (may be deprecated in the near future).	Allows for the management of Kubernetes clusters via the API	This permission is recommended for those who need to manage Kubernetes clusters via the API.	It is recommended this permission is set to None on the Tenant Role to restrict access for Subtenant users.

Virtual Desktop Permission Options

Permission Name	Permission Options	Feature Access	Description	Recommendations	Tenant Role Recommendations
Virtual Desktop: Copy/Paste	None, Full	Allows copy and paste access from the virtual desktop terminal	Enables the user to copy and paste values from a virtual desktop session into the paste buffer of their local computer		
Virtual Desktop: Local Printer	None, Full	Enables printing from a virtual desktop session to a locally installed printer			
Tools: VDI Pools	None, Read, Full	Allows for the management of virtual desktop (VDI) pools.	Enables the user to access the VDI Pools section (Tools > VDI Pools) and view existing pools (with “read” permission) or create and edit pools (with “full” permission). Related API functions are also granted with this feature permission.	This permission is recommended for those needing to manage VDI pools	

Users

Subtopics

- Users

Users

Subtopics

- Overview
- Create User
- Edit User
- User Settings

Overview

The Users page displays a list of all Users. The following fields are surfaced for each User:

- Display Name
- Username
- Email
- Role

Users which are grayed out in the list are currently inactive and cannot log in. The pencil and trash icons at the end of each row allow for editing or deleting Users. Click MORE to see the “impersonate” button. This allows administrators to impersonate any User, which may help confirm their Role permissions meet and do not exceed the desired result.

Click on the hyperlinked Display Name of the User to see a page detailing their effective Role permissions. This is especially useful for Users in multiple Roles where it might otherwise be difficult to determine their exact rights. This page looks identical to a User Role detail page except none of the fields are editable. Edit the User Role permissions for the User if changes need to be made.

NOTE

Some User data created through an Identity Source integration (such as Active Directory) is not editable in VM Essentials, as it is synced from the Identity Source.

Create User

About this task

Users are created in Administration > Users.

NOTE

Authorized Identity Source Users will be automatically created upon first sign in.

To create a User:

Procedure

1. Navigate to Administration > Users
2. Select + CREATE USER.
3. From the New User Wizard input:

   Username & Email

   - First Name
   - Last Name
   - Username
   - Email address

   Receive Notifications

   Enable to receive provisioning email notifications.

   Roles

   Role(s) to be inherited by the user. If multiple roles are selected, the higher permission levels of one role will override the other role(s). See the Roles section of this documentation for more information on stacking Roles and specific Role permissions.

   Password

   Password must contain at least one uppercase letter, one lowercase letter, a number, and a symbol.

   Enabled

   If unchecked, the user will no longer be able to sign into VM Essentials, but their user data will remain.

   Account Locked

   This box is checked when a User has tried unsuccessfully to log in too many times. An administrator will need to uncheck this box in order for the User to be able to make another login attempt.

   Password Expired

   If enabled, the User will be forced to create a new password upon next login. The expired password cannot be used again.

   Linux Settings

   Creates a User with the supplied Username, Password and/or Key-pair on Linux Instances when “Create my User” is selected during provisioning, or a User Group is added to an Instance of which this VM Essentials user is a member of.

   Windows Settings

   Creates a User with the supplied Username, Password and/or Key-pair on Windows Instances when “Create my User” is selected during provisioning, or a User Group is added to an Instance of which this VM Essentials user is a member of.

   IMPORTANT

   Please ensure password entered is allowable by Windows.

4. Select SAVE CHANGES.

Edit User

About this task

User settings can be edited from Administration > Users.

NOTE

Some User data from Users created via an Identity Source Integration such as Active Directory is not editable in VM Essentials, as it is synced with the Identity Source.

To edit a User from the Administration_>_Users Section:

Procedure

1. Select the Administration link in the navigation bar.
2. Select the Users link in the sub navigation bar.
3. Click the edit (pencil) icon from within the row of the selected User
4. Make changes and select SAVE CHANGES.

User Settings

Additional settings for a User can be found in the User Settings section, including a user photo, API access, two-factor authentication settings, default Groups and Clouds, and more. User Settings is accessed by clicking on the name of the User in the upper-right corner of the application window and selecting “User Settings.” See the dedicated section on User Settings elsewhere in this documentation for a more in-depth description of User Settings.

Health

Subtopics

VM Essentials Health
Logs

VM Essentials Health

The VM Essentials Health section provides an overview of the health of your VM Essentials appliance. It includes an appliance health summary in the following areas:

- **CPU:** Appliance CPU usage is checked. If usage is greater than 50%, this indicator will be in a yellow or warning state. If VM Essentials is unable to complete the check, it will be in a red or error state. Depending on appliance performance and how frequently this indicator is in a warning state, it may be necessary to upgrade to increase CPU. The **Overall** health indicator will mirror the CPU health indicator
- **Memory:** If swap usage is above 60% or VM Essentials memory usage is above 95%, this indicator will be in a yellow or warning state. If VM Essentials is unable to complete the check for any reason, it will be in a red or error state. Depending on appliance performance and how frequently this indicator is in a warning state, it may be necessary to increase swap, upgrade the appliance to add memory, or consider a different appliance architecture for those using single-node appliances
- **Storage:** If utilization of the filesystem mounted at “/” exceeds 80%, this indicator will be in a yellow warned status. Above 90% will put this indicator in red or error status
- **Database:** The database is checked. If the number of database connections exceeds the configured maximum number of connections or if any test queries are reported as being slow, this indicator will be in a yellow or warning state. If VM Essentials is unable to communicate with the database, it will be in a red or error state. In the database section further down the page, you can check the number of maximum used connections against the number of max connections. In the case of database connections exceeding the maximum, consider increasing the maximum settings connection

- **Elastic:** Elasticsearch is polled for the health status of each index. If any indices are not reporting a “green” health status, this indicator will be in a yellow or warning state.
- **Queues:** RabbitMQ queues are checked. Any queues containing more than 1000 messages are considered to be in an error state. Appliance Queue health is given in a yellow or warning status when any queues are in such an error state. In the Queues section further down the page you can see the individual Queues listed and which have messages piling up. When the appliance is unable to complete the check for any reason, this indicator will be in a red or error state

Subtopics

Health Levels
Additional System Health Indices

Health Levels

Health levels provide a live representation of the current memory and CPU load on the appliance. Bear in mind that in an HA appliance, this data will be specific to the appliance node you happen to be using. By default, VM Essentials does not include any endpoint or UI tool which can show you the currently used app node. However, a plugin has been developed which can surface this information if needed. See this thread in the VM Essentials official forums for additional details about accessing and using the plugin.

- **Morpheus CPU:** Instantaneous amount of CPU capacity in use by VM Essentials processes
- **System CPU:** Instantaneous amount of CPU capacity in use by all processes
- **Morpheus Memory:** Instantaneous amount of system memory currently in use by VM Essentials processes (see the Knowledge Base article linked in the TIP box below for more information on how VM Essentials claims and manages available memory)
- **System Memory:** Instantaneous amount of total system memory currently claimed (this is commonly a high percentage, see the TIP box below)
- **Used Swap:** Instantaneous amount of total available system swap in use
- **Storage:** The instantaneous percentage utilization of the filesystem mounted at “/”

Additional System Health Indices

CPU

- Processor Count
- Process Time
- Morpheus CPU
- System CPU
- System Load

MEMORY

- Morpheus Memory
- Morpheus Used Memory
- Morpheus Free Memory
- Morpheus Memory Usage
- System Memory

- System Used Memory
- System Free Memory
- System Memory Usage
- System Swap
- Free Swap

DATABASE

- Lifetime Connections
- Aborted Connections
- Max Used Connections
- Max Connections
- Threads Running
- Threads Connected
- Slow Queries
- Temp Tables
- Key Reads
- Handler Reads
- Buffer Pool Free
- Open Tables
- Table Scans
- Full Joins
- Key Read Requests
- Key Reads
- Engine Waits
- Lock Waits
- Handler Reads
- Engine IO Writes
- Engine IO Reads
- Engine IO Double Writes
- Engine Log Writes
- Engine Memory
- Dictionary Memory
- Buffer Pool Size
- Free Buffers
- Database Pages
- Old Pages
- Dirty Page Percent

- Max Dirty Pages
- Pending Reads
- Insert Rate
- Update Rate
- Delete Rate
- Read Rate
- Buffer Hit Rate
- Read Write Ratio
- Uptime

ELASTIC

- Status
- Cluster
- Node Count
- Data Nodes
- Shards
- Primary Shards
- Relocating Shards
- Initializing
- Unassigned
- Pending Tasks
- Active Shards

NOTE
status is typical for Elasticsearch

Elastic Nodes

- Node
- Master
- Location
- Heap Usage
- Memory Usage
- CPU Usage
- 1M Load
- 5M Load
- 15M Load

Elastic Indices

- Health
- Index

- Status
- Primary
- Replicas
- Doc
- Count
- Primary
- Size
- Total Size

Queues

- Queue Count
- Busy Queues
- Error Queues

Logs

The VM Essentials logs tab aggregates appliance-specific logs into one list. If needed, users can export the logs by clicking EXPORT. This action triggers a download containing the last 10,000 log entries as a `.log` file.

Settings

The Administration > Settings section sets global configuration parameters for the VM Essentials appliance, whitelabeling, provisioning, monitoring, backups, logs, software licenses, and the license for VM Essentials itself.

Subtopics

- Appliance
- Provisioning
- Backups
- Environments
- License
- Utilities

Appliance

Subtopics

- Appliance Settings
- Tenant Management Settings
- User Management Settings
- Email Settings
- Twilio SMS Settings
- Proxy Settings
- Currency Settings

Integrating With a Currency Exchange Provider
Consuming Currency Exchange in VM Essentials
Enabled Clouds (Types)

Appliance Settings

Appliance URL

The default URL used for Agent install and Agent functionality. All Instances and Hosts must be able to resolve and reach this URL over 443 for successful agent install and communication.

NOTE

Alternate Appliance URLs can be configured per Cloud in the Edit Cloud > Advanced Options section.

Internal Appliance URL (PXE)

For PXE-Boot your appliance needs to be routable directly with minimal NAT masquerading. This allows one to override the default appliance url endpoint for use by the PXE Server. If this is unset, the default appliance url will be used instead.

API Allowed Origins

A CORS-related field which specifies the origins that are allowed to access the VM Essentials API. For example, if you were designing a web application which needed to make AJAX calls to VM Essentials API. The origins should be specified here. By default, all origins are allowed. When this field is filled, an exclusive whitelist of allowed origins is established.

Cloud Sync Interval

Data is refreshed through cloud integrations at the interval specified here in seconds, the default value is 300 seconds (five minutes). Appliances managing a very large number of clouds may be adversely affected by setting this value too low.

Cluster Sync Interval

Data is refreshed through provisioned Clusters at the interval specified here in seconds, the default value is 60 seconds. Appliances managing a very large number of Clusters may be adversely affected by setting this value too low.

Usage Retainment

Determines how many days to keep account usage (metered costing data) records. Retainment period is not set by default. Usage records will remain indefinitely if Usage Retainment is not set. Note this does not affect generated Invoice records.

Invoice Retainment

Enter the number of days VM Essentials should keep invoice records in the database. In general, this setting can be left alone but in certain cases may need to be adjusted as very large invoice database tables can affect the stability of the application.

Incident Retainment

Enter the number of days VM Essentials should keep incident records in the database. In general, this setting can be left alone but in certain cases may need to be adjusted as very large incident database tables can affect the stability of the application.

Stats Retainment

Select 30, 60 or 90 days period for stats retainment. Selecting a larger period gives the ability to analyze stats, such as Instance metrics, over a longer period of time. For example, in the Monitoring tab of an Instance detail page, users can select a 60 or 90-day analysis period if the stats have been retained that long

Denied Hosts

A comma-delimited list of IP addresses and/or hostnames which should not be allowed sources for HTTP Tasks or REST-populated Option Lists.

Approved Hosts

A comma-delimited list of IP addresses and/or hostnames which are the only approved sources for HTTP Tasks or REST-populated Option Lists. By entering any values here, all others are automatically denied.

Exchange URL

Enter the URL which should be checked for updates to any installed plugins. The default exchange is: `https://share.morpheusdata.com`

Skip Agent Install

For appliances in which skipping the Agent install is the default selection, enable this global flag to default to skipping the Agent install during provisioning

Enable SSL Verification of Agent (Communications)

Enabling SSL Verification of Agent Communications requires a valid Certificate be installed on the Appliance.

Disable SSH Password Authentication

Only allow ssh login using SSH keys. When true, SSH Password Authentication will not be enabled for VM's and Hosts provisioned after the setting is enabled.

Default Appliance Locale

Sets the default language and region for all users on the VM Essentials appliance. Users with individual language preferences may also override this selection on their User Settings page

Default Console Gateway

Select a configured VM Essentials Worker as a console gateway or VDI gateway. For more on installation and configuration of a gateway, see the **VDI Gateways section** of VM Essentials documentation.

Max Option List Size

Sets a maximum size for Option Lists (such as those sourced from REST calls to a remote server) to preserve appliance performance in the event that a very large payload is inadvertently accessed. The entered number is multiplied by 1000 (for example, entering "1" results in a maximum list size of 1000).

Tenant Management Settings

Registration Enabled

If enabled, the appliance login screen will have a "NEED AN ACCOUNT? SIGN UP HERE" link added, enabling new Tenant registration.

Default Tenant Role

Sets the default Tenant Role applied to Tenants created from Tenant Registration.

Default User Role

Sets the default User Role applied to the User created from a Tenant Registration.

Docker Privileged Mode

Enable to allow Docker containers running on VM Essentials Docker hosts to run in privileged mode which adds additional access to the host hardware and resources but also comes with additional security risks

User Management Settings

Min Password Length

User passwords must at least be as many characters in length as the entered value

Min Password Uppercase

User passwords must include at least as many uppercase characters as the entered value

Min Password Numbers

User passwords must include at least as many numerals as the entered value

Min Password Symbols

User passwords must include at least as many special characters as the entered value

Session Expires (Minutes)

A user session is forcibly logged out after the entered number of minutes of inactivity

Session Warning (Minutes)

A pop-up warning is shown to the user when they have been inactive for the number of minutes entered. Example: If sessions are set to expire after 90 minutes, warn the user after 60 minutes if you intend to provide 30 minutes advance warning

Expire Password After (Days)

User account passwords will expire after the entered number of days. Enter 0 or leave the field empty to opt out of this feature.

Disable User After Attempts (Number of Attempts)

Disable a User account after a specified number of failed login attempts. Enter 0 or leave the field empty to opt out of this feature.

Disable User If Inactive For (Days)

Disable a User account if inactive for the entered number of days. The User will not be able to log into the appliance again until another User with sufficient rights enables the account. Enter 0 or leave the field empty to opt out of this feature.

Send warning email before deactivating (Days)

Enter the number of days prior to account deactivation that a warning email should be sent. For example, enter “5” to warn the User when they are five days short of the deactivation time entered in the prior field. Enter 0 or leave the field empty to opt out of this feature.

Email Settings

In this section, you can configure an SMTP server for email notification delivery. You will need to provide VM Essentials the following information, your mail server systems administrator can assist you in filling these fields and with the preferred encryption method.

- From Address
- SMTP Server
- SMTP Port
- SSL Enabled
- TLS Encryption
- SMTP User
- SMTP Password

We recommend that you add the VM Essentials server to your SMTP whitelist as well as using user authentication as an additional security measure.

Once you have added your SMTP server information into VM Essentials, scroll down to the bottom of the page and press the blue SAVE button which can be found under the Enabled Clouds section.

When you have saved your SMTP server settings in the VM Essentials appliance you will then need to restart the UI. To restart the morpheus-ui, connect to your VM Essentials server via SSH and run the below command:

```
sudo morpheus-ctl restart morpheus-ui
```

IMPORTANT

If you do not restart morpheus-ui, the notifications will not be sent. Please note it can take up to three minutes for the UI to become reachable again.

Twilio SMS Settings

Configure SMS text message delivery for VM Essentials alerts. Previously, customers could use VM Essentials’ own account for delivery, but

for security reasons clients must now supply their own. Complete the fields indicated below and then restart all VM Essentials nodes to apply the changes.

- **Account SID:** Twilio Account SID
- **SMS From #:** The “From” number to receive the text message from
- **Auth Token:** The Twilio API authentication token for your account

Proxy Settings

The VM Essentials Appliance can be configured to communicate through a Proxy server for Cloud API’s and Agent communication back to the Appliance.

> **NOTE**
> Additional Proxy configuration is available in the Infrastructure > Network > Proxies section. Added Proxies can be scoped to Clouds in the Edit Cloud > Advanced Options section of the Cloud.

Add a Global Proxy server by entering the following:

- Proxy Host
- Proxy Port
- Proxy User
- Proxy Password
- Proxy Domain
- Proxy Workstation
- No Proxy

Currency Settings

In VM Essentials, Tenants are separate environments which can be defined as using currencies that are unique from one Tenant to the next. In addition, these currencies may be different from the currency in which Price Sets have been defined. In order to present pricing to Subtenant users in their designated currency, VM Essentials allows for integration with currency conversion services “open exchange rates” and “fixer.io”. This article goes through the process of setting up the integration and how it works to determine pricing conversions.

Integrating With a Currency Exchange Provider

Procedure

1. Navigate to Administration > Settings > Appliance
2. Under the Currency Settings heading, make a “Currency Provider” selection
3. Enter your “Provider API Key”

Results

The service is now integrated and can be used as described in the next section.

Consuming Currency Exchange in VM Essentials

Currency exchange data is synced from the integrated provider once every 12 hours. When needed, Morpheus will use this cached data to present currency conversions rather than hitting the API directly each time. This limits the total number of API hits and reduces costs.

Exchanged currency values will be shown under conditions similar to the following scenario:

A user is working in a Subtenant configured for Currency B. The user is attempting to provision an instance with pricing sets that have only been defined in Currency A. Morpheus will convert the pricing data from currency A to Currency B for this user (and all users in this Subtenant) since price conversion has been enabled.

Enabled Clouds (Types)

Controls which types of Cloud can be created.

- When a Cloud type is disabled, it will be removed from the available options when adding new Clouds in Infrastructure > Clouds. Existing Clouds are not affected by changes to this setting.

Provisioning

Subtopics

Provisioning Settings
Cloud-Init Settings
Windows Settings
Library Settings
PXE Boot Settings
App Blueprint Settings
Terraform Settings

Provisioning Settings

Allow Cloud Selection

Displays or hides Cloud Selection dropdown in Provisioning wizard.

Allow Host Selection

Displays or hides Host Selection dropdown in Provisioning wizard.

Require Environment Selection

Forces users to select and Environment during provisioning

Hide Datastore Stats On Selection

Hides Datastore utilization and size stats in provisioning and app wizards

Cross-Tenant Naming Policies

Enable for the `sequence` value in naming policies to apply across tenants

Reuse Naming Sequence Numbers

When selected, sequence numbers can be reused when Instances are removed. Deselect this option and VM Essentials will track issued

sequence numbers and use the next available number each time.

Show Console Keyboard Layout Settings

When enabled Users will see keyboard layout settings in console sessions

Deployment Archive Store

Default Storage Provider for storing Deployment Archives.

NOTE

Storage Providers can be configured and managed in the Infrastructure > Storage section.

Cloud-Init Settings

VM Essentials can add global users for Linux and Windows at provision time. Cloud-init/Cloudbase-Init or VMware Tools installed on the provisioned virtual images is required.

Linux

- **Username:** Enter User to be added to Linux Instances during provisioning.
- **Password:** Enter password to be set for the above Linux user.
- **KeyPair:** Select KeyPair to be added for the above Linux user.

NOTE

Either a password, keypair, or both can be populated for the Linux user. Keypairs can be added in the Infrastructure > Keys & Certs section.

Windows Settings

- **Administrator Password:** Enter password to be set for the Windows Administrator User during provisioning.

Library Settings

In this section, enable or disable access globally to provisioning sections of Catalog (self-service shopping cart provisioning), Apps (apps deployed from configured App Blueprints), and Instances

- Enable Catalog
- Enable Apps
- Enable Instances
- Provisioning Order: Sets the order for Instances, Apps, and Catalog to appear in the Provisioning menu

PXE Boot Settings

Default Root Password

Enter the default password to be set for Root during PXE Boots.

App Blueprint Settings

Determines the Default Blueprint Type selected in new App Wizard

- Morpheus
- ARM Template
- CloudFormation
- Terraform
- Kubernetes Spec
- Helm Chart

Terraform Settings

- **Terraform Runtime:** Select “auto” or “manual”. When selecting “auto”, VM Essentials will automatically download and use the Terraform version indicated in the VERSION field on the Spec Templates that make up a Terraform Instance type or Blueprint. When selecting “manual”, VM Essentials will use the version of Terraform **installed on your appliance**.

Backups

Subtopics

Backup Settings

Backup Settings

The Backup settings page allows you enable or disable scheduled backups, select a default backup bucket, and administer global settings related to backups. Changes to global settings only affect new backups going forward and do not affect existing backups.

NOTE

Appliance backups are subject to a two-hour time limit to complete the backup. Automated backup attempts will be abandoned and will fail once this time limit is exceeded.

Subtopics

VM Essentials Backup Settings

VM Essentials Backup Settings

Scheduled Backups

Enable automatic scheduled backups for provisioned instances

Create Backups

When enabled, VM Essentials will automatically configure instances for manual or scheduled backups

Backup Appliance

When enabled, a backup will be created for the VM Essentials appliance database. Select the `Backup` text link to view or edit settings related to the appliance backup

Default Backup Bucket

Select an existing bucket as the default for future backup runs. Click the `Infrastructure Storage` text link to add a new storage bucket to VM Essentials if needed

Default Backup Schedule

Choose a default schedule interval for automated backups. The available selections in this dropdown menu are Execution Schedules defined in Library > Automation > Execute Scheduling

Default Backup Retention

Choose the default number of backups to be retained for automated Instance and appliance backup jobs

Default Synthetic Full Backup enabled

When enabled, full synthetic backups will be on by default in addition to standard backups for supported workload types

Default Synthetic Full Backup Schedule

Choose a default schedule interval for full synthetic backups. The available selections in this dropdown menu are Execution Schedules defined in Library > Automation > Execute Scheduling

Environments

Subtopics

Overview

Overview

The Environments section is where you create and manage your environment labels, which are available in the Environment dropdown during Instance or App provisioning. An Instance's environment label can be changed by editing the Instance.

Subtopics

Creating Environments

Creating Environments

Procedure

1. Select + Create Environment
2. Populate the following for the New Environment:

Name

The friendly name for the environment in VM Essentials

Code

Shortcode used for API and CLI

Description

Environment description displayed on the Environments list page

Display Order

The order in which environments are presented when provisioning, a value of “0” will position the environment at the top of the list

Results

NOTE

User-created environments can be edited, hidden, or removed from the Actions menu on the environments list page. VM Essentials-default environments can only be hidden from users during provisioning.

License

Subtopics

Overview
Current License
Upgrade License Key

Overview

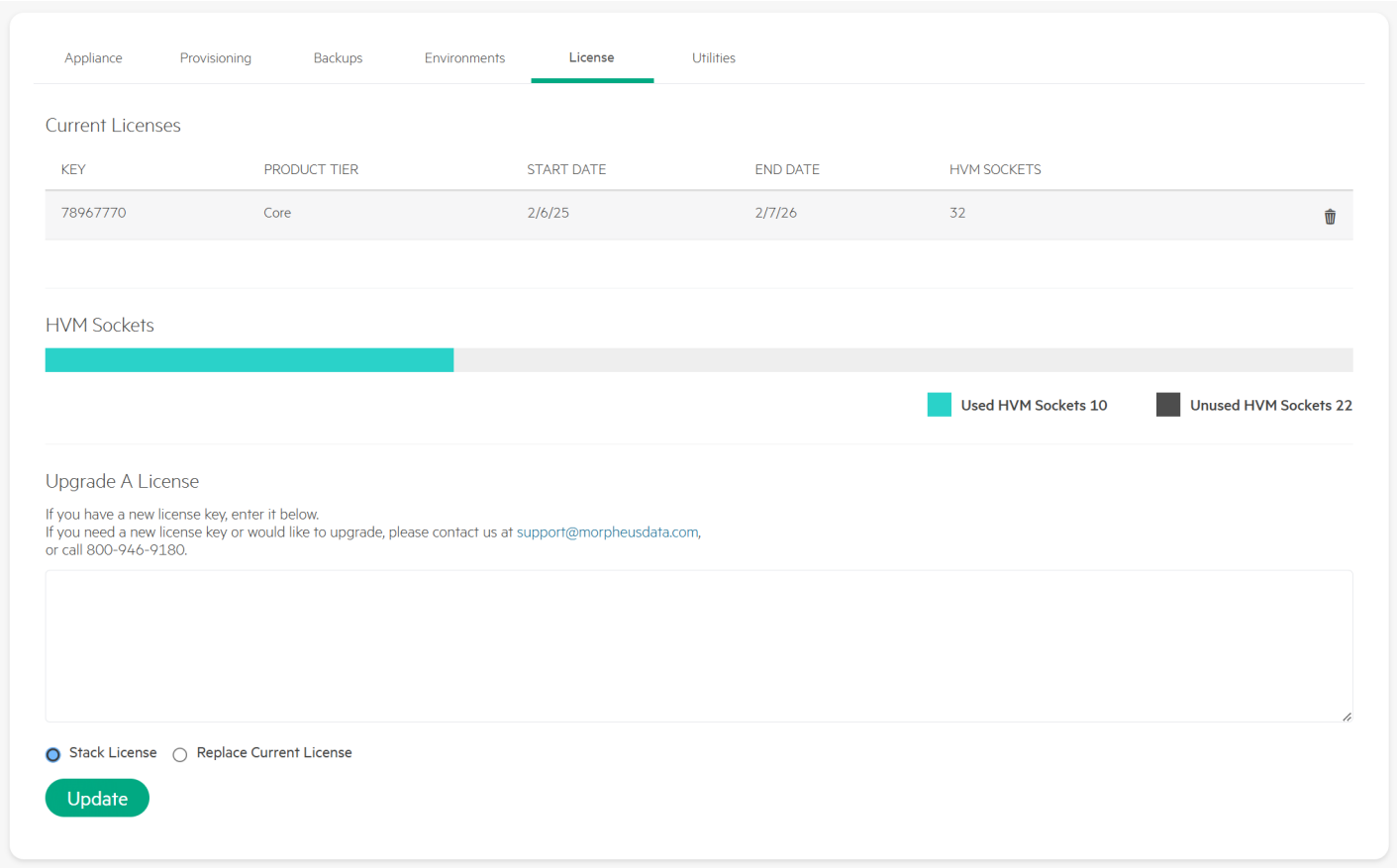
VM Essentials requires a valid license for provisioning new Instances and Clusters, and converting existing Instances to managed. Licenses can be applied and updated in this section, and the current license status, as well as usage metrics, can be checked.

Current License

If a License Key has already been applied, it will be shown in the list of Current Licenses. This page also contains useful information on license usage including start and end dates for the license, the total number of HVM sockets licensed, and how many of the licensed HVM sockets have been used.

NOTE

Once a current License expires or has reached its limits, users will no longer be able to provision new Instances or Clusters and will not be able to convert existing VMs to managed. HPE Morpheus VM Essentials will otherwise continue to function.



Upgrade License Key

About this task

To add a new or update an existing License:

Procedure

1. Copy the license key into the large text area at the bottom of the page
2. Click UPDATE

Results

If valid, the new License will be applied. Note that the new license may replace an existing license or may stack onto an existing license.

Utilities

System administrators have access to a utilities panel with the following options:

- **Reindex all searchable data:** Execute
- **Toggle Maintenance Mode:** Enable

NOTE

Maintenance mode cleanly places VM Essentials into a state where maintenance can be performed on the appliance. This drains any active sessions and queues so an auto-scaling group can scale down. It also drains active sessions across services. Restarting VM Essentials UI disables maintenance mode.

NOTE

When using VM Essentials in a Highly Available (HA) environment, it is important to navigate to a node directly and enable maintenance mode, as opposed to using the load balancer virtual IP (VIP). A local host entry to the specific node may be required to ensure the correct node enters mainteance mode. In fact, it is recommended to use the **analogous API endpoint** to toggle a specific node into maintenance mode to avoid redirects back to the VIP address.

A VM Essentials node in maintenance mode can still be accessible through the load balancer VIP/target group and can queue requests but will not process anything in queue, while in maintenance mode. A node can be removed/paused from the load balancer VIP or have VIP health checks implemented, if the node UI/API will become inaccessible due to maintenance.

User Settings

User settings are accessed by clicking on your display name in the far upper-right corner of the application window. In this dropdown menu, click on the “USER SETTINGS” link.

Subtopics

- User Photo
- User Settings
- 2 Factor Authentication
- Preferences
- Linux Settings
- Windows Settings
- API Access

User Photo

Upload a custom image for your user avatar that is displayed in the top header and user administration sections. **Suggested Photo Dimensions: 128 x 128**

User Settings

The fields included in this section are described below. By entering any new values in these fields and clicking SAVE, the existing value will be overwritten.

- **Theme:** Choose from a selection of themes including default and dark mode themes. The Theme setting is not available when Whitelabeling is enabled on the current Tenant
- **Username:** Your VM Essentials username
- **First Name:** Your first name (together with Last Name makes up your display name)
- **Last Name:** Your last name (together with First Name makes up your display name)
- **Email:** Your email address

- **Password:** Enter a value and save changes to update your password. The value in the Confirm field below must match
- **Confirm:** Confirm the new password you've entered
- **RECEIEVE NOTIFICATIONS** Determines if provisioning notifications are emailed to this User

2 Factor Authentication

VM Essentials supports two-factor authentication (2FA) for local user accounts as well as those authenticating through Active Directory and LDAP identity sources. Authentication is handled through a 2FA app such as Authy or Google Authenticator. Other common methods for handling 2FA, such as through email or SMS text message are not currently supported. Two-factor authentication is handled on a per-user basis through the User Settings section. There is not currently a way for an administrator to enforce the use of two-factor authentication appliance-wide.

Subtopics

Setting Up Two-Factor Authentication
Disabling Two-Factor Authentication
Handling User Lock-Out

Setting Up Two-Factor Authentication

When two-factor authentication isn't yet set up, this section contains a single button: ENABLE 2FA. To get started, click this button and VM Essentials will prompt for your password. After entering the password, you'll be shown a QR code which can be scanned into your authenticator application of choice. Once the QR code is shown, 2FA is active and the supplemental code will need to be entered each time the user logs in.

On subsequent login attempts, the user will be prompted to enter a 2FA code after successful entry of the username and password. Retrieve this code from the 2FA app you set up in the prior section and enter it to complete the login process.

Disabling Two-Factor Authentication

When two-factor authentication is set up, this section contains two buttons: DISABLE 2FA and GET 2FA CODE. To generate a new QR code and configure an authenticator app, click GET 2FA CODE. Once you generate a new QR code, the old one is no longer valid. At that point you must reconfigure your authenticator app or you will not be able to access your account on the next login attempt. Generating a new QR code requires your password.

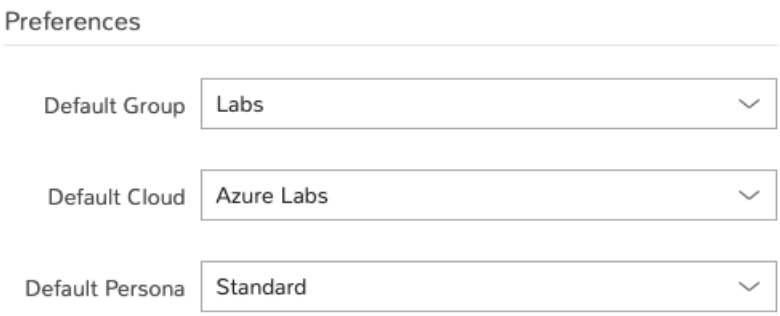
To disable 2FA, click DISABLE 2FA. This action does not require a password.

Handling User Lock-Out

If a user loses the device they've configured for authentication or if they cannot proceed through 2FA login for any other reason, an administrator should impersonate the user's account, reset their password, disable 2FA, then share the new temporary password with the user. At that point, the user can login, reset their password to something more secure, and re-enable 2FA (if desired).

Preferences

- **Default Group:** Sets the default Group selection when provisioning
- **Default Cloud:** Sets the default Cloud selection when provisioning
- **Default Persona:** Sets the default Persona used when logging in
- **Default Locale:** Sets the user's preferred language and region, this setting will override the global locale for the individual user



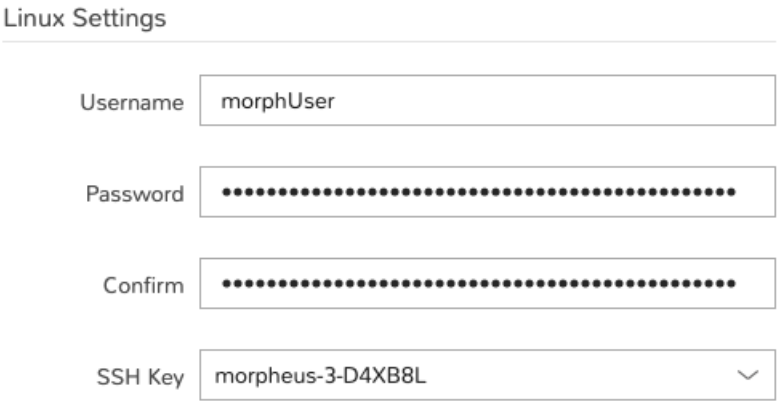
Linux Settings

When provisioning a Linux-based resource and opting to have your user created during the provisioning process, the credentials entered in this section will be used to seed that user into the provisioned resource.

- **Username:** The username that will be used with your Linux user
- **Password:** The password that will be used with your Linux user (optional if specifying key)
- **Confirm:** Confirm your entered password. These must match in order for the new password value to be saved
- **SSH Key:** Select a pre-existing SSH key pair object in Morpheus. Required of not specifying password and creating your user during provisioning, or required if ssh password authentication has been disabled.

WARNING

If your users Linux Settings password and/or key are not defined, and 'Create User" is enabled during provisioning (default), a random password will be generated but not exposed and you will not be able to login with your user.



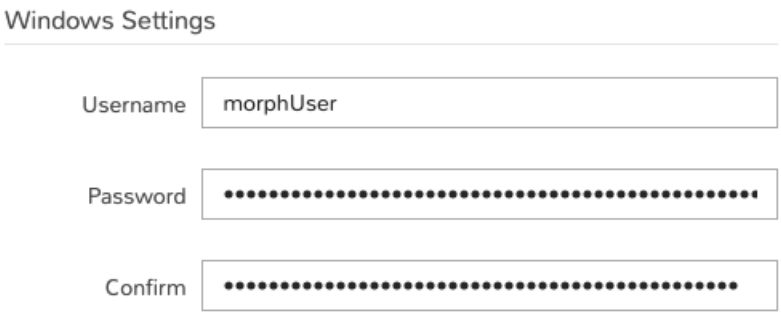
Windows Settings

When provisioning a Windows-based resource and opting to have your user created during the provisioning process, the credentials entered in this section will be used to seed that user into the provisioned resource.

- **Username:** The username that will be used with your Windows accounts
- **Password:** The password that will be used with your Windows accounts
- **Confirm:** Confirm your entered password. These must match in order for the new password value to be saved

WARNING

If your users Windows Settings password is not defined, and 'Create User" is enabled during provisioning (default), a random password will be generated but not exposed and you will not be able to login with your user.



API Access

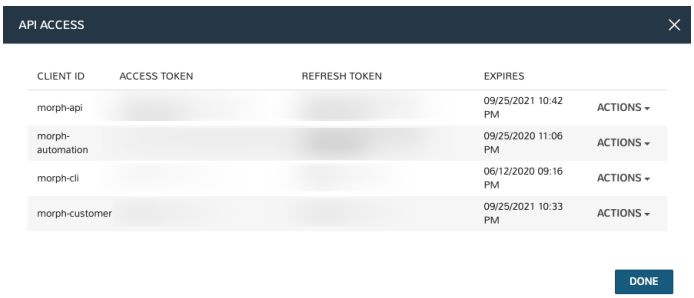
Click the API Access button to expand the "API ACCESS" modal. In this modal you can generate or refresh access tokens that can be used with Morpheus API and Morpheus CLI.

If no token yet exists for a particular "CLIENT ID", click ACTIONS and then Generate. If a token has expired, we can also regenerate that token by clicking ACTIONS and then Regenerate. After regenerating a particular token, you would need to ensure any scripts using those tokens are updated.

- **morph-api:** Used for VM Essentials API access and should be the default token-type used

- **morph-cli:** Used for VM Essentials CLI access
- **morph-automation:** Used by the internal Task engine and by jRuby-type Tasks to make API calls. It shouldn't be used externally for other types of access or in external automation. It is surfaced in the UI so users can see if a token exists and can clear it when necessary
- **morph-customer:** This token is available for legacy implementations and was previously recommended for custom API access (similar to the morph-api token). It's not recommended for use but is still available to maintain support for legacy custom automation which may still be in use on customer sites

After navigating away from the User Settings page, the complete access and refresh tokens will be masked from view. If these are lost or compromised, you can eliminate a token completely by clicking ACTIONS and then Clear. If you need to generate a new token for the same Client ID, click ACTIONS and then Regenerate.



NOTE

Access Tokens are only displayed/available after generation. Copy new Tokens and store appropriately before navigating from `/user-settings`, they will not be displayed again.

Guides

Subtopics

- Integration Guides

Integration Guides

Subtopics

- Clouds
- Networking Integrations
- Storage
- Image preparation

Clouds

Subtopics

- VMware vCenter

VMware vCenter

Subtopics

- Overview
- Features
- Getting Started
- Windows Provisioning Tips
- Existing Instances
- Service Plans
- Virtual Images / Blueprints
- Snapshots
- Affinity Groups
- Tagging and Metadata
- Advanced
- VMware Permissions
- Creating a VM Essentials VMware Image
- Creating a CentOS/RHEL 7 Image
- Creating a CentOS/RHEL 8 Image
- Gotchas
- A Note on Proxies

Overview

VMware is a very common cloud integration choice supported by VM Essentials . They have provided a top notch virtualization solution and one might argue pioneered the virtualization space altogether. As such, many companies utilize this technology and all the features that come with it, so VM Essentials covers a broad feature set in vCenter.

Features

- Virtual Machine Provisioning
- Backups / Snapshots
- Resource Groups
- Datastores and DRS Clusters
- Distributed Switches
- Datacenter / Cluster scoping
- Brownfield VM management and migration
- VMware to VMware migrations
- VMDK/OVF image conversion support
- Hypervisor Remote Console
- Periodic Synchronization
- Veeam Backup Integration
- Lifecycle Management and Resize
- Metadata tag sync

On top of all these features, VM Essentials also adds additional features to VMware that do not exist out of the box to make it easier to manage in multitenant environments as well as hybrid cloud environments:

- Cloud-Init Support
- VHD to VMDK Image Conversion
- QCOW2 to VMDK Image Conversion
- Multitenancy resource allocation
- Virtual Image management (Blueprints)
- Auto-scaling and recovery

Getting Started

To get started with VMware, simply start by adding a Cloud in the Infrastructure > Clouds section.

To start adding a VMware cloud there will be some things you will need:

vCenter API Url

Typically this is the url to the vCenter web client with a `/sdk` in the path

Username/Password

A set of credentials with high level access to VMware (ensure the account has Datacenter level access)

Once these fields are entered, some selections will start pre-populating. A cloud integration is scoped to a specific data center, and can optionally be scoped down to a single cluster or even a single resource pool. If the drop downs do not populate, please verify the api url is resolvable, morpheus has access to vCenter on 443, and the provided credentials are correct and the user has sufficient permissions.

Another cool feature provided with the cloud integration is optional Resource Pool scoping. One can choose to allow the cloud to provision into All Resource Pools or a singular Resource Pool. When choosing All, these Resource Pools can be managed from a sub-account and visibility perspective via the Cloud Detail page (multi-tenancy).

The VMware cloud integration provides a few additional options including allowing users to make host selections or keeping that aspect hidden such that the best host is automatically chosen for the requested provision.

The *RPC Mode* feature can be configured to allow VM Essentials to install its agent on the Guest operating system via either SSH/WinRM or Vmware Tools Guest Process feature. The VMware tools Guest Execution API can be tricky so it is recommended to use SSH/WinRM if possible. However, if it is not possible for the Appliance to have outbound access to all networks in which VMs are being provisioned to the SSH/WinRM ports (22, 5985 respectively) then Guest Execution is the only option.

The Use VNC console option on the VMware cloud requires special configuration on each ESXI host but allowed hypervisor level remote console support. (See the Advanced Section for details)

When following this add cloud wizard an option will be presented to create a group or add to an existing group. These groups can be given provisioning permission via role based access control. It is normally recommended that groups are organized such that one cloud exists in one group unless the networks are setup such that internal routing is possible between the clouds. This is very useful for bursting, or hybrid cloud configurations.

Windows Provisioning Tips

By default when provisioning windows templates, VM Essentials performs guest customizations which initiates a sysprep. This resets the Administrator user and password. VM Essentials will set the Administrator password from Administration > Settings > Provisioning > Windows Settings > Password.

Users can also set the username on an image as Administrator and enter a different password if unique passwords are required per image.

Guest customizations are required when assigning static IP's manually or using IP pools. They can be disabled per virtual image advanced settings under Library > Virtual Images > Edit Image > Advanced > Uncheck "Force Guest Customization" if using DHCP. However the SID will not be changed from the source template. In addition, new VM's will not be able to join a domain that had already been joined by the source template or any other VM's with that SID.

Existing Instances

VM Essentials provides several features regarding pulling in existing virtual machines and servers in an environment. Most cloud options contain a checkbox titled '*Inventory Existing Instances*'. When this option is selected, all VMs found within the specified scope of the cloud integration will be scanned periodically and Virtual Machines will be synced into VM Essentials. Users may also choose to onboard only virtual machines that are running within specific Resource Pools. Once the vCenter Cloud is integrated, navigate to the detail page for the specific Cloud (select it from the list at Infrastructure > Clouds). From the Resources tab, locate the Pools section. Click ACTIONS > Editnext to a selected Resource Pool. If INVENTORY is checked, VM Essentials will automatically onboard virtual machines from that Resource Pool.

By default these virtual machines are considered 'unmanaged' and do not appear in the Provisioning > Instances area but rather Infrastructure > Compute > Virtual Machines. However, a few features are provided with regards to unmanaged instances. They can be assigned to various accounts if using a multitenant master account, however it may be best suited to instead assign the 'Resource Pool' to an account and optionally move all servers with regards to that pool (more on this later).

A server can also be made into a managed server. During this process remote access is requested and an agent install is performed on the guest operating system. This allows for guest operations regarding log acquisition and stats. If the agent install fails, a server will still be marked as managed and an Instance will be created in Provisioning, however certain features will not function. This includes stats collection and logs.

NOTE

All Cloud data is resynchronized on a 5 minute interval. This includes Datastores, Resource Pools, Networks, Blueprints, and Virtual Machines.

Service Plans

A default set of Service Plans are created in VM Essentials for the VMware provisioning engine. These Service Plans can be considered akin to AWS Flavors or Openstack Flavors. They provide a means to set predefined tiers on memory, storage, cores, and cpu. Price tables can also be applied to these so estimated cost per virtual machine can be tracked as well as pricing for customers. By default, these options are fixed sizes but can be configured for dynamic sizing. A service plan can be configured to allow a custom user entry for memory, storage, or cpu. To configure this, simply edit an existing Service Plan tied to VMware or create a new one. These all can be easily managed from the Admin > Plans & Pricing section.

Virtual Images / Blueprints

VM Essentials will automatically take an inventory of all blueprints configured in vCenter and present them as options during provisioning. However, in order for VM Essentials to properly provision these virtual machines and provide accurate stats and health of these virtual machines, an agent must be installed during virtual machine startup. This means remote access needs to be granted at the guest operating system level to VM Essentials . To properly configure these virtual images, find the relevant images in Library > Virtual Images and edit the entry. On this form, a few options are presented. The first is a check box asking whether or not cloud-init is enabled. If cloud-init is enabled, simply provide the default OS username configured (for Ubuntu the username is ubuntu and for CentOS the username is centos). For those looking to add cloud-init to existing blueprints VM Essentials requires no special configuration and can use the default cloud.cfg settings.

A global cloud-init username/password can also be configured per account as well as a keypair via the `Admin->Provisioning` settings section. The great benefit of utilizing cloud-init is default blueprints do not need common credential sets thereby increasing provisioning security.

Windows systems do not typically support cloud-init. So simply turn this checkbox off and provide the Administrator credentials. It should be noted that these credentials are encrypted in the database. If using WinRM for the RPC Mode instead of VMware tools, a Local or Domain Administrator account credential set can be provided instead.

Snapshots

VM Essentials allows the ability to create a snapshot of a VM in VMware vCenter. From the instance detail page, simply select Actions > Create Snapshot to begin creation of a new Snapshot. Existing snapshots can be viewed in the BACKUPS tab on the instance detail page. Snapshots taken in vCenter will sync into VM Essentials every five minutes. To revert to a previous snapshot, click on the revert icon located on the right side of the Snapshot. Snapshots can be deleted by clicking on the trash can icon.

NOTE

Access to Snapshots can be limited or removed entirely for specific user roles as needed. To edit a role's Snapshots permissions, go to Administration > Roles > (Your selected role) > Snapshots. Users can be given Full, Read-only, or No access.

IMPORTANT

VM Essentials supports the use of SR-IOV network adapters with VMware Clouds. Bear in mind that VMware does not support Snapshots for this network adapter type and for that reason Snapshot and backup-related features will also fail in VM Essentials for VMs using SR-IOV network adapters.

Affinity Groups

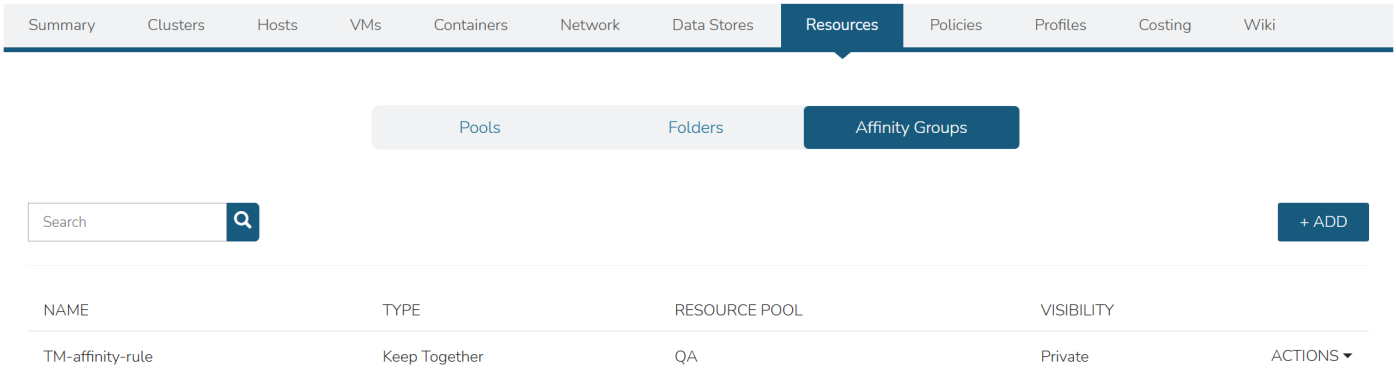
HPE Morpheus VM Essentials Software offers two-way sync for affinity groups with integrated VMware vCenter Clouds. An affinity group contains a type (either Keep Together or Keep Separate) and a list of servers which should have the rule applied. Affinity groups created from HPE Morpheus VM Essentials create "Should" rules (soft rules) rather than "Must" rules (hard rules) in vCenter. Thus whenever possible, servers configured to "Keep Together" will run on the same cluster host while servers configured to "Keep Separate" will be balanced across cluster hosts to the maximum extent possible. These rules may be broken if necessary to balance resources or recover from failures.

TIP

It is possible to create an empty affinity group (that is, one with no servers selected) in HPE Morpheus VM Essentials even though this is not possible in vCenter. If such an affinity group is created, HPE Morpheus VM Essentials will hold it without syncing to vCenter until at least one server is added and the affinity group becomes compatible with the vCenter API.

Viewing Affinity Groups

Affinity groups are listed on the Resources tab of the Cloud detail page (Infrastructure > Clouds, then select the appropriate VMware Cloud). From the ACTIONS menu for each affinity group, they may be edited or deleted. By editing an affinity group, users may view or edit its enabled status (affinity groups which are not enabled will not be acted on).



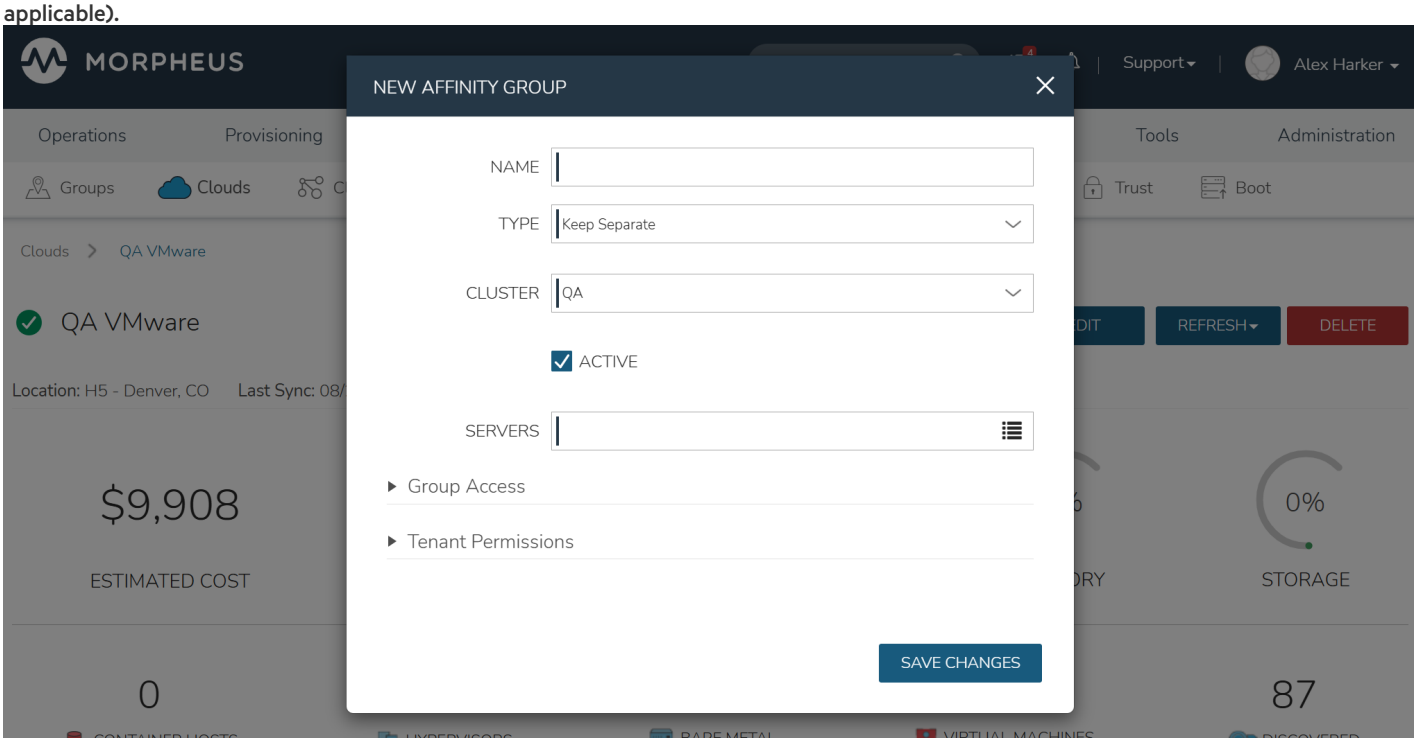
Adding Affinity Groups

As mentioned in the previous section, affinity groups are listed on the Resources tab of the VMware Cloud detail page (Infrastructure > Clouds, then select the appropriate VMware Cloud). From here, to create a new affinity group, click + ADD. Configure the following:

- **NAME:** A name for the affinity group
- **TYPE:** Select either "Keep Together" or "Keep Separate" to indicate whether the selected servers should run on as few or as many servers as possible within the capabilities of the HVM Cluster

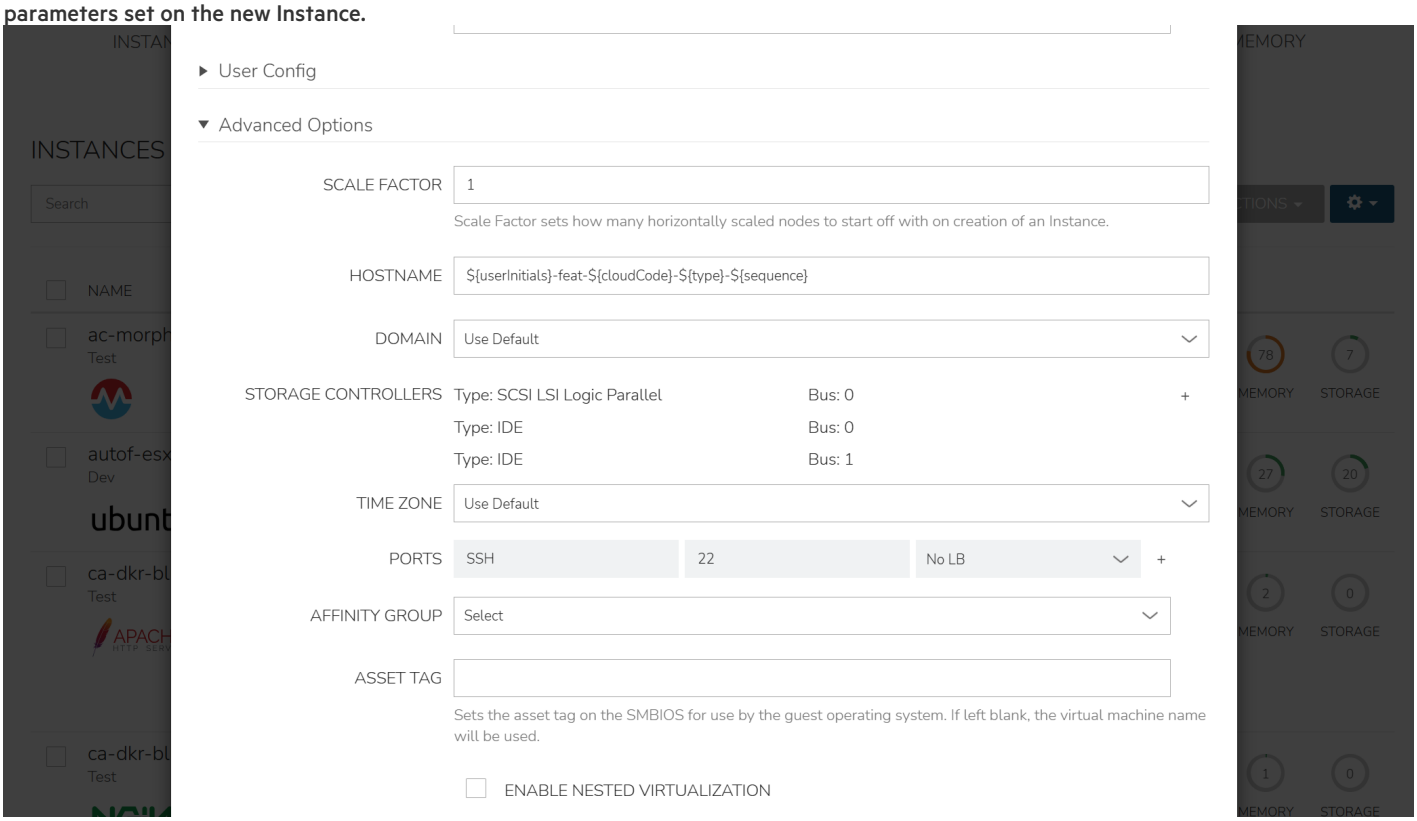
- **CLUSTER:** Select the vCenter cluster
- **ACTIVE:** When checked, the rules defined in the affinity group will be applied to the HVM Cluster
- **SERVERS:** Select as many servers as desired from the typeahead list

Once finished, click SAVE CHANGES. Following the next Cloud sync, the affinity rule will be applied and VMs will begin to migrate (if applicable).



Adding Servers to Affinity Groups at Provision Time

In addition the adding servers from the affinity group, newly-provisioned servers may be added to an affinity group at provision time. From the CONFIGURE tab of the provisioning wizard, expand the Advanced Options section. Within Advanced Options, select an affinity group. The affinity group must be pre-existing and this list will be filtered to show only affinity groups that apply depending on other configuration parameters set on the new Instance.



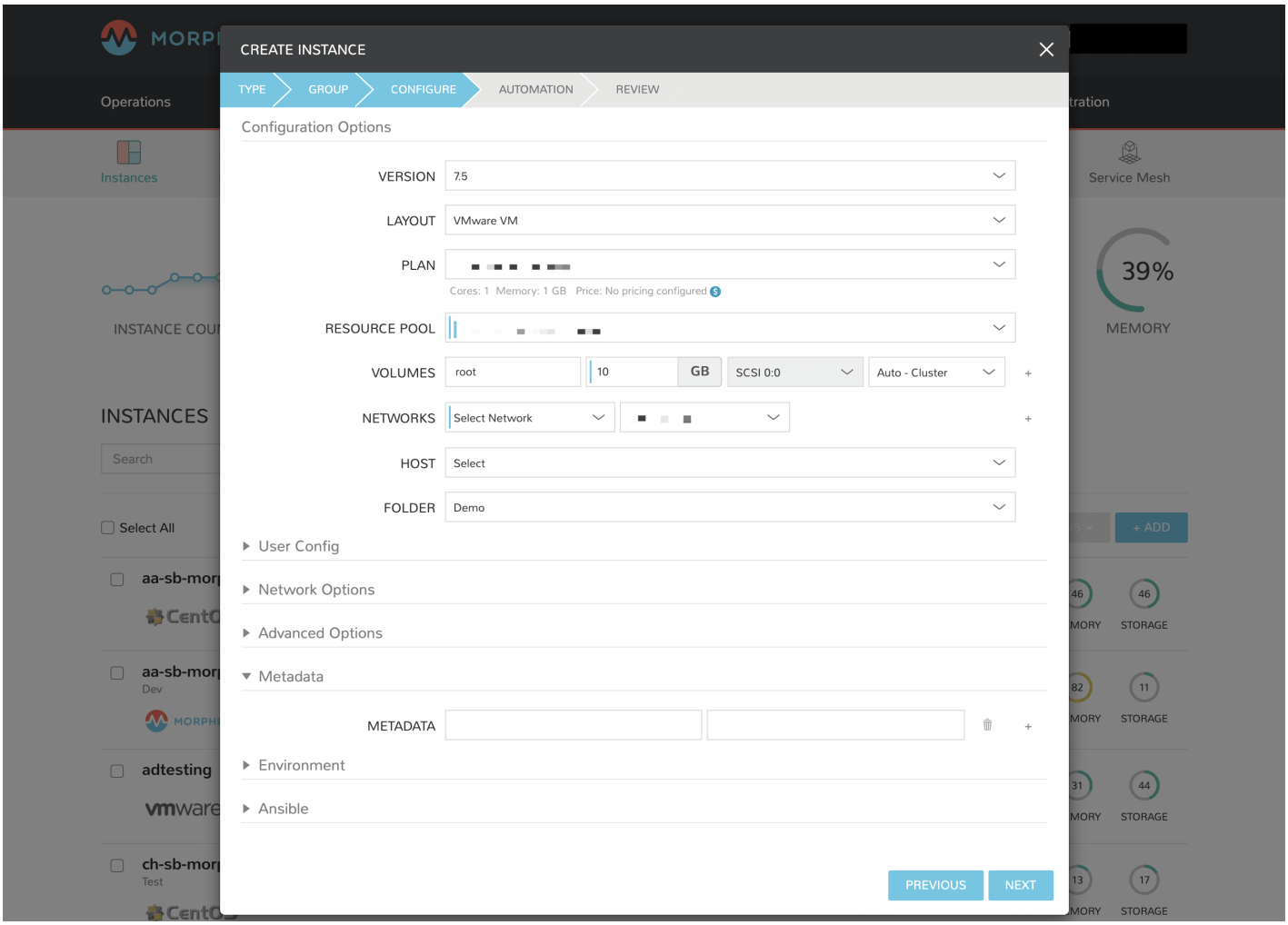
Tagging and Metadata

As of Morpheus version 4.1.0, tagging support is included for vCenter in addition to the other clouds that have already supported it in past versions. Tags will sync to vCenter from Morpheus and existing tags are also inventoried from vCenter into Morpheus.

> **NOTE**
>
> This feature requires a minimum API version of vCenter 6.5. The API version can be edited by navigating to 'Infrastructure > Clouds' and clicking the edit (pencil) button in the row for the relevant cloud. The field is labeled 'VERSION'.

Tags can be created on-demand when provisioning from the 'CONFIGURE' tab of the 'CREATE INSTANCE' wizard (Provisioning > Instances). Within the 'Metadata' drawer, you will see sets of fields to enter key/value pairs. On creation of the instance, this metadata will be synced into vCenter.

'Inputs' from your library can also be exported as metadata for use with vCenter. When adding or editing a new Input (Library > Options > Inputs), simply mark the box labeled 'EXPORT AS METADATA'. The 'FIELD NAME' becomes the tag category in VMWare.



Advanced

There are several advanced features provided within VM Essentials that can leverage some cool aspects of VMware. One of these features is Remote Console support directly to the hypervisor. To enable this feature a few prerequisites must be met. First, the VM Essentials appliance must have network access to the ESXi hosts within VCenter. Secondly, firewall settings need to be adjusted on each ESXi host. This can be done in VSphere under firewall configuration on the host. Simply check the gdbserver option, which will open up the necessary

ports (starting at 5900 range).

> **IMPORTANT**
> Hypervisor Console for vCenter 6.5 requires VM Essentials v3.2.0+

Now that the ESXi hosts are ready to utilize remote console, simply edit the cloud in VM Essentials via Infrastructure > Clouds. Check the option that says Enable Hypervisor Console. It is important to note that currently this functionality only works for newly provisioned vm's provisioned directly via VM Essentials. This should change soon however.

It is also possible to import vm snapshots for backup or conversion purposes from VCenter and also an ESXi host. However, this does require that the ESXi host license has an enterprise level license as it will not allow the appliance to download a virtual image if it is not a paid VMware license.

VMware Permissions

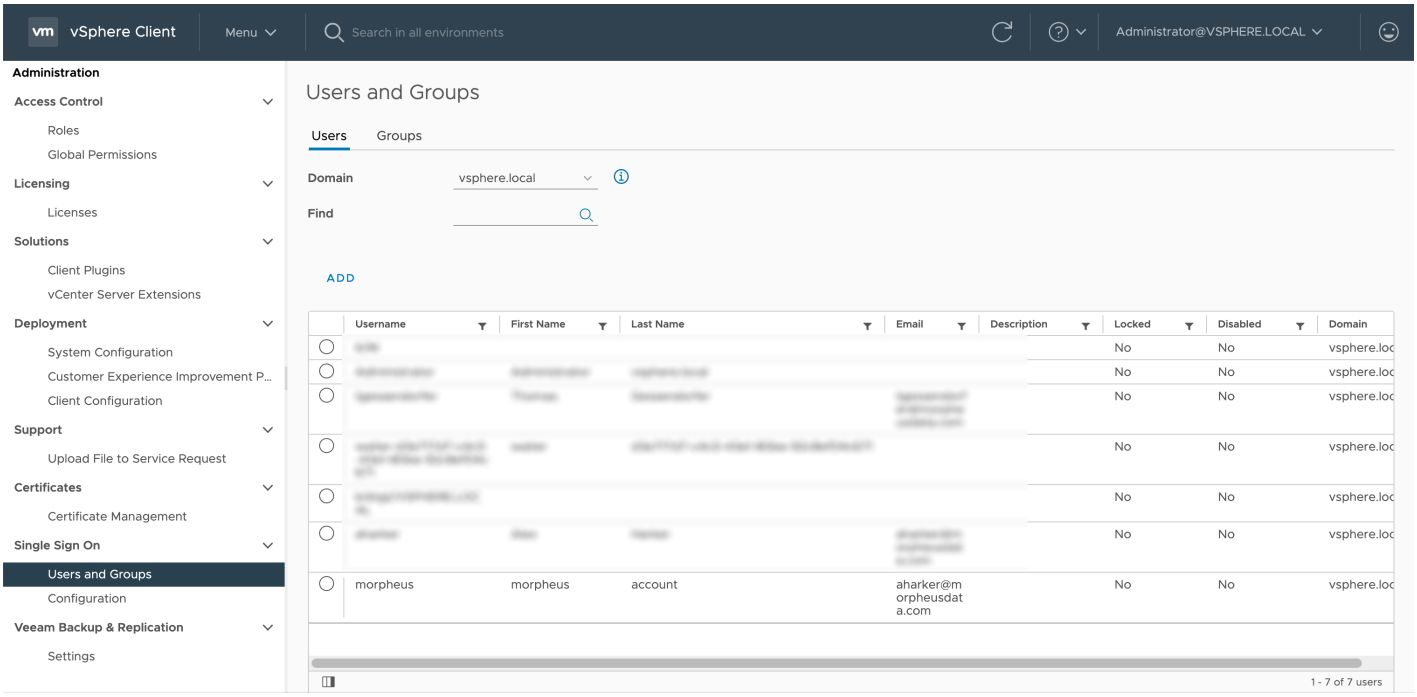
When integrating VMware vCenter with VM Essentials, users must supply credentials for a vCenter account and VM Essentials will only have access privileges equal to the integrated account. Many users will choose to use a vCenter administrator account so that VM Essentials can freely do any function in vCenter without worrying about hitting access limits. Others, for security reasons, may want to restrict VM Essentials only to the minimum permissions it needs to perform its functions. Follow the guide in this section to configure a user with minimal permissions and associate it with the appropriate usage levels before using it to create a VM Essentials Cloud integration.

Subtopics

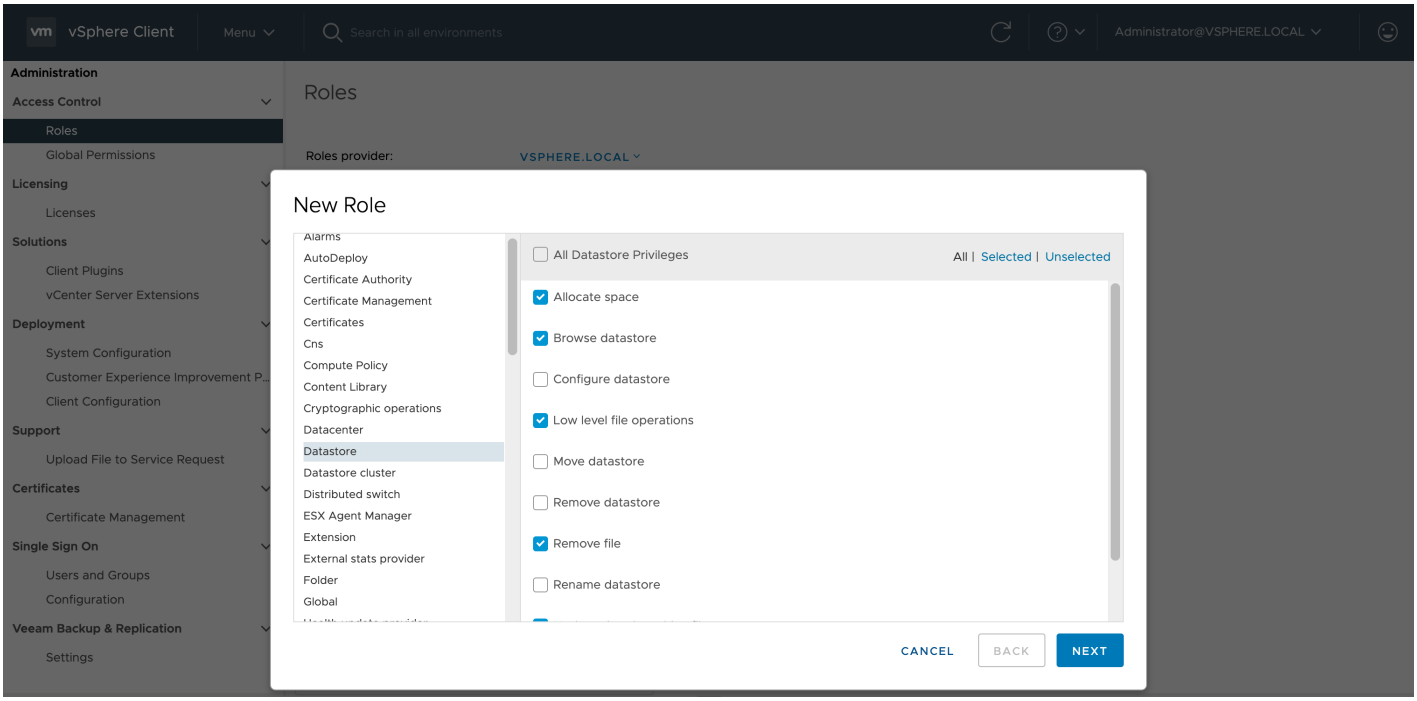
- Create vCenter Users and Roles
- Privileges
- Usage

Create vCenter Users and Roles

For this example, I've added a new local user to be my VM Essentials integration user (Menu > Administration > Users and Groups) but any existing user, whether locally-created or sourced from an identity integration (like Active Directory), works fine.



The next step is to create a Role (Menu > Administration > Roles). You can edit an existing Role to be sure it has the correct privileges, I've opted to create a new role and assign the correct privileges. Below the screenshot, take note of the complete set of required privileges. Once all privileges are set, name the Role (if it's a new one) and click Finish.



Privileges

Content Library

- All Content Library privileges

Datastore/Datastore Cluster

- Allocate Space
- Browse Datastore
- Low Level file Operations
- Remove File
- Update virtual machine files
- Update virtual machine metadata

Distributed Switch

- Port configuration operation
- Port setting operation

Global

- Log Event
- Manage custom attributes
- Set custom attribute

Network

- Assign Network
- Configure
- Remove

Resource

- Apply recommendation
- Assign vApp to resource pool
- Assign virtual machine to resource pool
- Migrate powered off virtual machine
- Migrate powered on virtual machine

Scheduled task

- Create tasks
- Modify task
- Remove task
- Run task

Tasks

- Create task
- Update task

Virtual Machine

- Configuration (all)
- Guest Operations (all)
- Interaction (all)
- Inventory (all)
- Provisioning (all)
- Service configuration (all)
- Snapshot management (all)
- vSphere Replication (all)

vApp

- Clone
- Export
- Import

vSphere Tagging

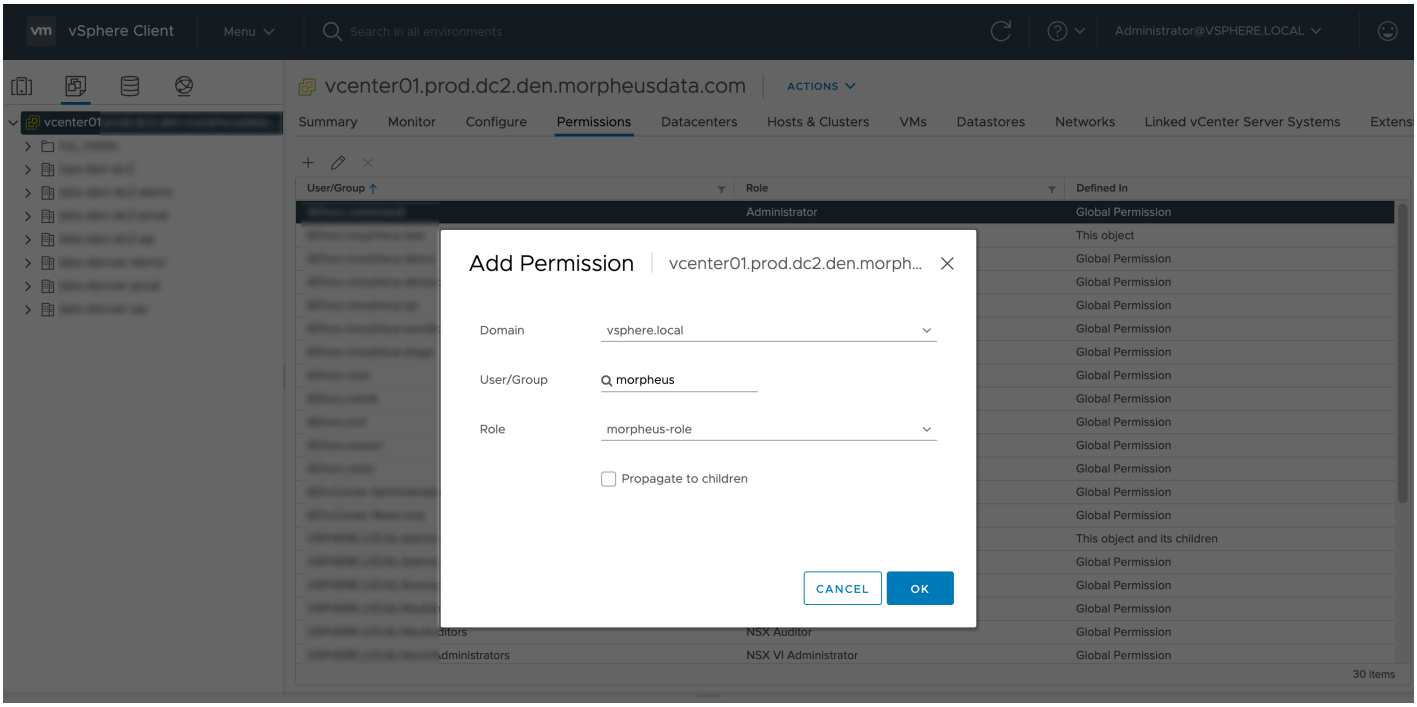
- Assign or Unassign vSphere Tag
- Assign or Unassign vSphere Tag on Object
- Create vSphere Tag
- Create vSphere Tag Category
- Delete vSphere Tag
- Delete vSphere Tag Category
- Edit vSphere Tag
- Edit vSphere Tag Category
- Modify UsedBy Field For Category

- Modify UsedBy Field For Tag
- privilege.InventoryService.Tagging.CreateScope.label
- privilege.InventoryService.Tagging.DeleteScope.label

With the User and Role created, add permissions to associate the User and Role to the appropriate usage constructs. Navigate to the usage construct you wish to work with, navigate to the permissions tab, click the plus (+) button. In the screenshot below, I'm adding the permission for the vCenter usage construct. The complete list of usages and whether or not to mark the propagation box is below the image.

NOTE

For organization and security purposes, permissions can also be added to folders. This allows VM Essentials to see the folders and onboard any resources within them (if desired). Once the vCenter Cloud integration has been created in VM Essentials, you can view folders from the Cloud Detail Page (Infrastructure > Clouds > Selected Cloud > ResourcesTab). By editing the folder here (Actions > Edit), folders can be set as the "Default" and/or the "Image Target". When a folder is set as Default, this folder is pre-selected when provisioning new Instances into the Cloud. When a folder is set as the Image Target, VM Essentials will look into this folder to onboard VMware images into VM Essentials.



Usage

vCenter

- Non-Propagating

Datacenter

- Non-Propagating

Cluster

- Non-Propagating

Host

- Non-Propagating

Datastore/Datastore Cluster

- Propagating

After completing the above steps, all VMware Cloud functionality should be available in VM Essentials without running into permissions errors.

Creating a VM Essentials VMware Image

VM Essentials comes out of the box with a default set of blueprints for use in many modern deployment scenarios. These consist mostly of base operating system images with a few additional adjustments. These adjustments typically include the addition of cloud-init (which is highly recommended to be used in most environments, but not mandatory). However, in many on-premise deployments there are custom image requirements as well as networking requirements. This guide will go over how to create a VMware Images for use within VM Essentials.

NOTE

A VM Essentials appliance may have many vCenter Clouds tied to any number of vCenter appliances. If the same images need to be available to multiple vCenter Clouds, you will need to download the OVF from one vCenter and upload it into the others. At that point you can make multiple VM Essentials Node Types from the images and it will be available to all needed vCenter Clouds. This is a vCenter limitation but one which may not be obvious when provisioning via VM Essentials.

Creating a CentOS/RHEL 7 Image

About this task

Create a new virtual machine in VMware vCenter and install a base version of your preferred Linux distro build. If you are using cloud init as part of your image you will need to ensure your virtual machine has a cdrom.

Procedure

1. Before installing the operating system setup a single `ext` or `xfs` partition without a swap disk (This is so that growpart can extend the disk. growpart currently does not support lvm)
2. Install the distro and apply any updates to the operating system and security updates
3. Install cloud-init using command `yum install cloud-init`
4. Install cloud-utils-growpart using command `yum install cloud-utils-growpart`
5. Install open-vm-tools using command `yum install open-vm-tools`
6. Install git by running `yum install git`
7. Install epel-release repo using command `yum install epel-release`
8. selinux set to permissive (enforced can cause problems with cloud-init) `sudo vi /etc/selinux/config`

Subtopics

Cloud-Init
Network Interfaces

Cloud-Init

To get started with a base CentOS image we first install cloud-init. This is a relatively simple process using yum:

```
yum -y install epel-release
yum -y install git wget ntp curl cloud-init dracut-modules-growroot
rpm -qa kernel | sed 's/^kernel-//'  | xargs -I {} dracut -f /boot/initramfs-{}.img {}
```

There are two parts to this yum installation. We are first ensuring some core dependencies are installed for automation as well as cloud-init. git for example is installed for use by ansible playbook automation down the line and is therefore optional if not using ansible. The dracut-modules-growroot is responsible for resizing the root partition upon first boot to match the virtual disk size that was potentially adjusted during provisioning.

A great benefit to using cloud-init is credentials don't have to be locked into the blueprint. It is advisable, within VM Essentials , to configure the default cloud-init user that gets created when the vm boots automatically by cloud-init. This is located in Administration > Settings > Provisioning, within the Cloud-Init Settings section.

Network Interfaces

A slightly annoying change with centOS 7 is that the network interfaces have changed naming convention. You may notice when running ifconfig that the primary network interface is set to something like ens2344 or some other random number. This naming is dynamic typically by hardware id and we don't want this to fluctuate when provisioning the blueprint in various VMware environments. Fortunately, there is a way to turn this functionality off and restore the interface back to eth0.

Firstly we need to adjust our bootloader to disable interface naming like this.

```
sed -i -e 's/quiet/quiet net.ifnames=0 biosdevname=0/' /etc/default/grub
grub2-mkconfig -o /boot/grub2/grub.cfg
```

The above command adds a few arguments to the kernel args list (namely `net.ifnames=0` and `biosdevname=0`. It may be useful to view the `/etc/default/grub` file and ensure these settings were indeed applied.

The next step is to adjust the network-scripts in centOS. we need to ensure we have a file called `/etc/sysconfig/network-scripts/ifcfg-eth0`

Below is a script that we run on our packer builds to prepare the machines network configuration files.

```
export iface_file=$(basename "$(find /etc/sysconfig/network-scripts/ -name 'ifcfg*' -
not -name 'ifcfg-lo' | head -n 1)")
export iface_name=${iface_file:6}
echo $iface_file
echo $iface_name
sudo mv /etc/sysconfig/network-scripts/$iface_file /etc/sysconfig/network-
scripts/ifcfg-eth0
sudo sed -i -e "s/$iface_name/eth0/" /etc/sysconfig/network-scripts/ifcfg-eth0
sudo bash -c 'echo NM_CONTROLLED=\"no\" >> /etc/sysconfig/network-scripts/ifcfg-
eth0'
```

This script tries to ensure there is a new ifcfg-eth0 config created to replace the old ens config file. Please do verify this config exists after running. If it does not you will have to be sure to build one on your own.

```
TYPE=Ethernet
DEVICE=eth0
NAME=eth0
ONBOOT=yes
NM_CONTROLLED="no"
BOOTPROTO="dhcp"
DEFROUTE=yes
```

Creating a CentOS/RHEL 8 Image

Create a new virtual machine in VMware vCenter and install a base version of your preferred Linux build. You must be running ESXi 6.7

Update 2 or later.

Subtopics

- Prepare The New CentOS 8/RHEL8 Image
- SELinux Settings
- Network Interfaces
- Final VMWare Tasks
- Creating an Ubuntu 20.04 Image

Prepare The New CentOS 8/RHEL8 Image

Procedure

1. Install epel-release: `yum -y install epel-release` (This step is not necessary for RHEL)
2. Install git, wget, curl, cloud-init, cloud-utils-gropart, and open-vm-tools: `yum -y install git wget curl cloud-init cloud-utils-growpart open-vm-tools`
3. Update: `yum -y update`
4. Finally run: `rpm -qa kernel | sed 's/^kernel-//' | xargs -I {} dracut -f /boot/initramfs-{}.img {}`

SELinux Settings

About this task

If allowed by your internal IT policies, set SELinux to permissive to avoid potential issues with cloud-init down the road.

Procedure

1. Edit the following: `vi /etc/selinux/config`
2. Make the following change: `setenforce 0`

Network Interfaces

About this task

Run the following to rename the network NIC. Values inside angle brackets should be filled in with the appropriate value for your environment (ex. <varname>):

Procedure

1. `sed -i -e 's/quiet/quiet net.ifnames=0 biosdevname=0/' /etc/default/grub`
2. `grub2-mkconfig -o /boot/grub2/grub.cfg` (location may be different, could be located at /boot/efi/EFI/centos/grub.cfg)
3. `ifdown <orginal-nic>`
4. `mv /etc/sysconfig/network-scripts/<orginal-nic> /etc/sysconfig/network-scripts/ifcfg-eth0` (this changes name/device to eth0)
5. Edit `ifcfg-eth0` and change the NAME to `eth0`

6. `bash -c 'echo NM_CONTROLLED=\"no\" >> /etc/sysconfig/network-scripts/ifcfg-eth0'`
7. `ip link set <orginal-nic> down`
8. `ip link set <orginal-nic> name eth0`
9. `ip link set eth0 up`
10. `ifup eth0`

Final VMWare Tasks

Procedure

1. Detach any install media
2. Shutdown the VM
3. Convert the VM to template on the VM Essentials side
4. Refresh the VM Essentials Cloud to allow the new template to sync

Creating an Ubuntu 20.04 Image

Download the Ubuntu 20.04 ISO from Canonical, and upload the base image to vCetner. Then, create a new virtual machine in vCenter.

NOTE

Since we'll include cloud-init with our image, we will need to ensure the virtual machine has a cdrom. Select the Ubuntu 20.04 ISO we just downloaded from the CD/DVD drive dropdown menu when creating the new virtual machine.

Before installing the operating system, set up a single ext partition without a swap disk. Then, continue on installing Ubuntu making the following selections during the setup process:

- Update to the latest installer if a later version is available
- Use the entire disk and deselect the option to set up the disk as an LVM group
- Configure an account and set a password
- Opt to install OpenSSH Server
- Other optional packages aren't needed for this basic Ubuntu image

Complete the installation process and reboot the machine. Update the package list and apply any upgrades:

```
apt-get update
apt-get upgrade
```

Change the network interface to `eth0` by editing `/etc/default/grub`. The line `GRUB_CMDLINE_LINUX=""` should be edited to `GRUB_CMDLINE_LINUX="net.ifnames=0 biosdevname=0"`.

Update GRUB:

```
update-grub
```

Update the `70-persistent-net.rules` file:

```
cat << EOF > /etc/udev/rules.d/70-persistent-net.rules
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{dev_id}=="0x0",
```

```
ATTR{type}=="1", NAME="eth0"
EOF
```

Remove `subiquity-disable-cloudinit-networking.cfg` as cloud-init will skip network configuration if it's present:

```
rm -f /etc/cloud/cloud.cfg.d/subiquity-disable-cloudinit-networking.cfg
```

Update `99-pve.cfg`:

```
cat << EOF > /etc/cloud/cloud.cfg.d/99-pve.cfg
datasource_list: [ConfigDrive, NoCloud]
EOF
```

Remove Netplan files, they will not be regenerated if they exist:

```
rm -f /etc/netplan/00-installer-config.yaml
rm -f /etc/netplan/50-cloud-init.yaml
```

Run cloud-init clean:

```
cloud-init clean
```

Next, reboot the system and confirm the network interface is labeled `eth0` once the machine comes back up. Then, clear BASH history for root. The history entry has a copy in the memory and it will flush back to the file when you log out. You can avoid this with the following command:

```
cat /dev/null > ~/.bash_history && history -c && exit
```

Shutdown the system:

```
shutdown -h now
```

Convert the VM to a template in vCenter before moving back to VM Essentials to onboard the image and use it to begin building your provisioning library.

Gotchas

SELinux can cause issues with cloud-init when in enforced mode. It may be advisable to set this to permissive unless it is mandatory within your organization to use an enforced SELinux configuration. If that is the case please see the documentation for the cloud_init_t security policies.

Network Manager will also prevent the required restart of the Network Service when assigning static IP's. Disable Network Manager when possible or Static IP assignment may not work until the Network Service is restarted manually.

A Note on Proxies

Proxy configurations are known to vary in some organizations and makes building a base blueprint a little more difficult. In order to fully configure proxies a few environment variables must be set in the /etc/environment file (This can be done automatically in a default user-data script for cloud-init as well in edit cloud).

```
http_proxy="http://myproxyaddress:8080"
https_proxy="http://myproxyaddress:8080"
ftp_proxy="http://myproxyaddress:8080"
no_proxy=127.0.0.1,localhost,applianceUrl
https_no_proxy=127.0.0.1,localhost,applianceUrl
```

IMPORTANT

It is very important to properly set the no_proxy list (applianceUrl) should be replaced with the actual appliance url. In future releases, morpheus plans to automatically take care of this.

NOTE

If using cloud-init agent install mode these settings need to be set in the custom Cloud-Init User data section of “Edit Cloud” or “Edit Virtual Image”

IMPORTANT

If using this virtual machine as a docker host, proxy settings must also be configured in the docker config. See Docker guides for instructions on how to properly set this. If necessary this can be wrapped in a task automation workflow for your own use.

Networking Integrations

Subtopics

- ArubaCX Network Integration
- HPE Aruba CX DSS

ArubaCX Network Integration

Subtopics

- Overview
- Features
- Prerequisites
- Adding ArubaCX Integration
- Add ArubaCX Integration to a Cluster

Overview

The ArubaCX network plugin is implemented as a VM Essentials `GenericIntegrationProvider` in Groovy. The plugin handles network and cluster events generated by VM Essentials and modifies the configuration of ArubaCX switches based on the cable connections between the affected servers and switches. VM Essentials integrates directly with ArubaCX to create or delete networks for OVS Port Groups that are added or deleted within a configured Cluster.

Features

- Network - Create or Delete OVS Port Group.

Prerequisites

- A pair of ArubaCX 8325 series switches
- All the hosts in the Cluster are connected to these pair of switches

- REST API access to the ArubaCX switches with administrative rights
- User credentials for the ArubaCX switch pair with API access granted and read/write access to the switch configuration

Subtopics

Server Network Configuration (Netplan)
Switch Configuration

Server Network Configuration (Netplan)

Procedure

1. On each host, configure a `bond0` interface on the management interfaces
2. The management interfaces should be connected to the ArubaCX switch pair Sample configuration:

```
{
   bonds:
     bond0:
       interfaces:
         - ens2f0np0
         - ens1f0np0
       parameters:
         mode: "active-backup"
   ...
}
```

Switch Configuration

Procedure

1. Configure the management interface and IP address on both switches in the pair
2. The switch pair must be configured with `vsx-sync` enabled for high availability and redundancy

   Sample configuration:

```
vsx
   inter-switch-link lag 256
   role primary
   keepalive peer 192.168.0.1 source 192.168.0.0
   vsx-sync loop-protect-global mclag-interfaces vsx-global
```

```
vsx
   inter-switch-link lag 256
   role secondary
   keepalive peer 192.168.0.0 source 192.168.0.1
   vsx-sync loop-protect-global mclag-interfaces vsx-global
```

3. Create a Multi-Chassis Link Aggregation Group (MC-LAG) between the ArubaCX switch and the upstream network, referred to as `lag 1`
4. Configure the `lag1` interface on both switches in the pair Sample configuration:

```
interface lag 1 multi-chassis
```

```
no shutdown
no routing
vlan trunk native 1
vlan trunk allowed 1,175
lacp mode active
loop-protect
```

5. The switch ports connected to the server's management interfaces should be set to "Trunk mode" with a "Native VLAN" Sample configuration:

```
interface 1/1/1
no shutdown
no routing
vlan trunk native 175
vlan trunk allowed 175
```

Adding ArubaCX Integration

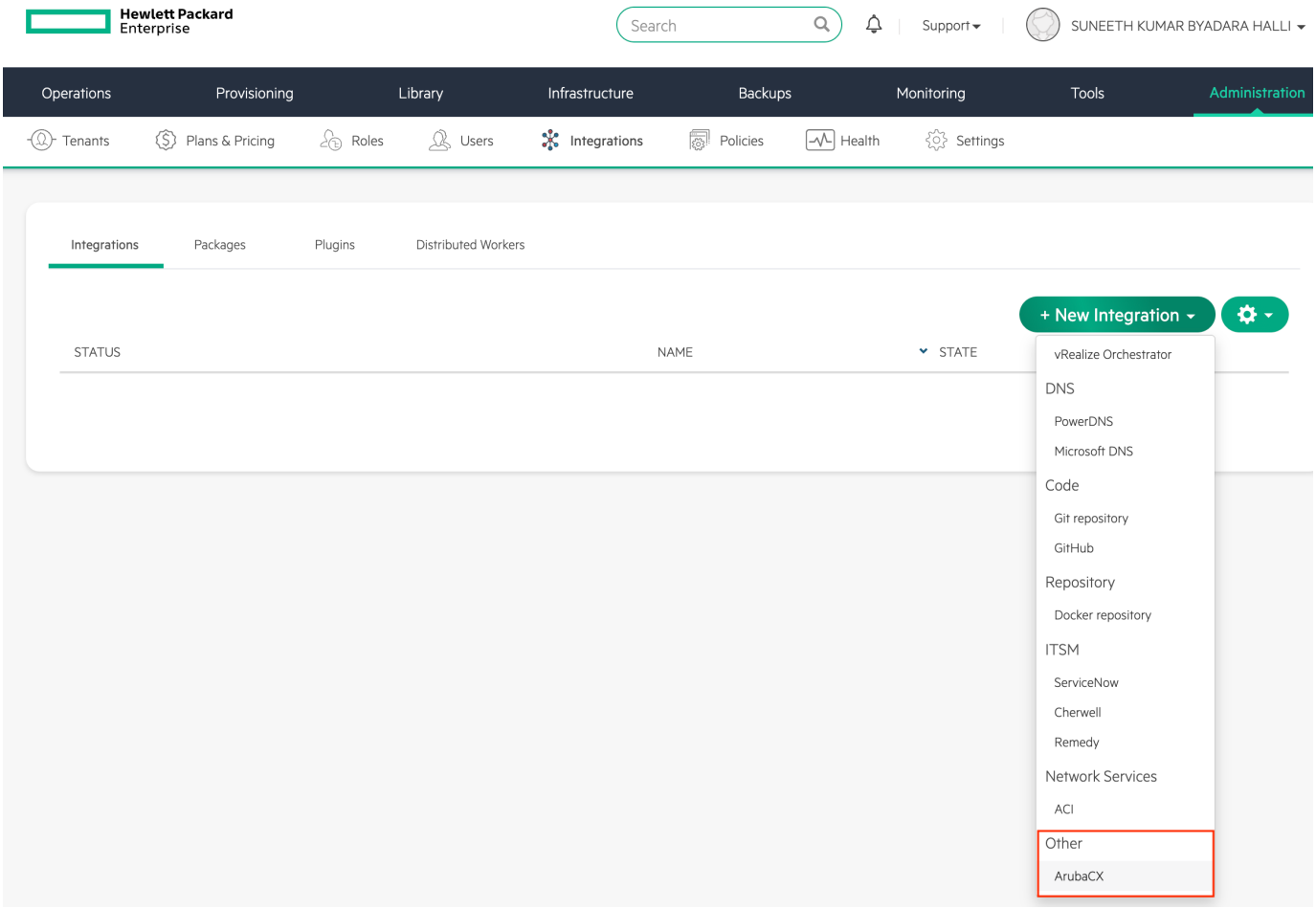
About this task

NOTE

Making full use of the HPE Morpheus VM Essentials ArubaCX integration requires credentials for Aruba CX switch pair with API access granted and read/write access to switch configuration. See ArubaCX 8325 documentation for more information on user rights administration in that product.

Procedure

1. Navigate to Administration > Integrations
2. Select + New Integration > Other > ArubaCX



3. Enter the following:

NAME

Name of the integration in HPE Morpheus Enterprise

ENABLED

Deselect to disable the integration

USERNAME

User username for all switches

PASSWORD

User password for all switches

IPV4 ADDRESS

Primary switch IP address for switch pair 1

IPV4 ADDRESS

Secondary switch IP address for switch pair 1

IPV4 ADDRESS

Primary switch IP address for switch pair 2

IPV4 ADDRESS

Secondary switch IP address for switch pair 2

IPV4 ADDRESS

Primary switch IP address for switch pair 3

IPV4 ADDRESS

Secondary switch IP address for switch pair 3

IPV4 ADDRESS

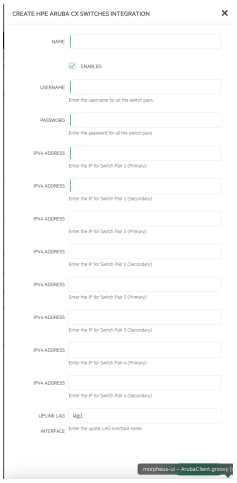
Primary switch IP address for switch pair 4

IPV4 ADDRESS

Secondary switch IP address for switch pair 4

UPLINK LAG INTERFACE

Name of the uplink LAG interface (default is 'lag1')



4. Select SAVE CHANGES

Results

Upon save the ArubaCX Network integration will be created.

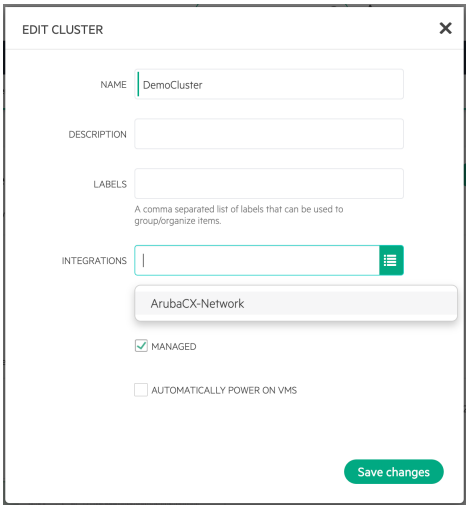
NOTE

All fields can be edited after saving.

Add ArubaCX Integration to a Cluster

Procedure

1. In Infrastructure > Clusters select the target Cluster
2. Select the Edit icon for the Cluster
3. In the “Integrations” dropdown, select an available ArubaCX Integration
4. Save Changes



HPE Aruba CX DSS

Subtopics

- Overview
- Features
- Prerequisites
- Adding HPE Aruba CX DSS Network Integration
- Create HPE ANW DSS Port Group Network
- Delete HPE ANW DSS Port Group Network
- View HPE Aruba CX DSS Network Integration

Overview

The HPE Aruba CX DSS plugin brings advanced networking features to HPE Morpheus VM Essentials Software by leveraging Aruba CX 10000 series switches. It supports both micro-segmentation and macro-segmentation, integrating seamlessly with HPE and Aruba technologies to improve user experience and operational efficiency.

Implemented as a VM Essentials `NetworkProvider` in Groovy, the plugin is purpose-built for the HPE Aruba Networking Distributed Services Switch network type (HPE ANW DSS Port Group) and optimized for VM Essentials environments. It automates the creation and management of networks for HPE ANW DSS Port Groups, connecting servers to Aruba CX 10000 switches within a HVM cluster.

On each host, the plugin creates Linux bridge interfaces and associates them with VLANs for streamlined network management and configuration. VM Essentials integrates directly with Aruba Fabric Composer (AFC) to automatically create or delete networks for HPE ANW DSS Port Groups as they are added to or removed from a configured cluster. Adding or removing HVM hosts in the HVM cluster triggers the corresponding network changes in AFC, ensuring the network configurations are always up to date.

The plugin also enables the creation of networks with specific VLAN IDs, supporting flexible segmentation and isolation. When a network is created, the plugin provisions the required VLANs on the Aruba CX 10000 switches, ensuring networks are ready for use by Instances within the HVM cluster.

Additionally, the plugin creates a Libvirt network of type Private. When an Instance is created on the host and associated with this network, a macvtap interface is generated and mapped to the corresponding Linux Interface VLAN ID, ensuring seamless connectivity and isolation.

Features

- Create and delete networks of type `HPE ANW DSS Port Group` directly from the integration

- Automatically create and delete networks in Aruba Fabric Composer (AFC) when HVM hosts are added or removed from the HVM cluster
- Manage network configurations through seamless integration with AFC
- Enable both micro-segmentation and macro-segmentation for flexible network isolation
- View detailed summaries and status of Aruba CX 10000 switches
- Ensure automatic, realtime synchronization of network configurations with Aruba CX 10000 switches

Prerequisites

The following requirements must be met to deploy and configure the HPE Aruba CX DSS Network plugin in VM Essentials

- Aruba CX 10000 series switches
  - At least two Aruba CX 10000 switches are configured
  - VSX and KeepAlive are configured
  - Switches are connected to the upstream network
- Pre-existing HVM cluster
  - Ensure all hosts within the HVM cluster are physically connected to the CX 10000 switches for optimal network integration and redundancy
- VM Essentials appliance version 8.0.6 or higher
  - AFC and PSM are deployed and reachable from the VM Essentials manager
- Aruba Fabric Composer (AFC) version 7.2 or higher, deployed as a VM
- AMD Pensando PSM (Policy and Services Manager), deployed as a VM

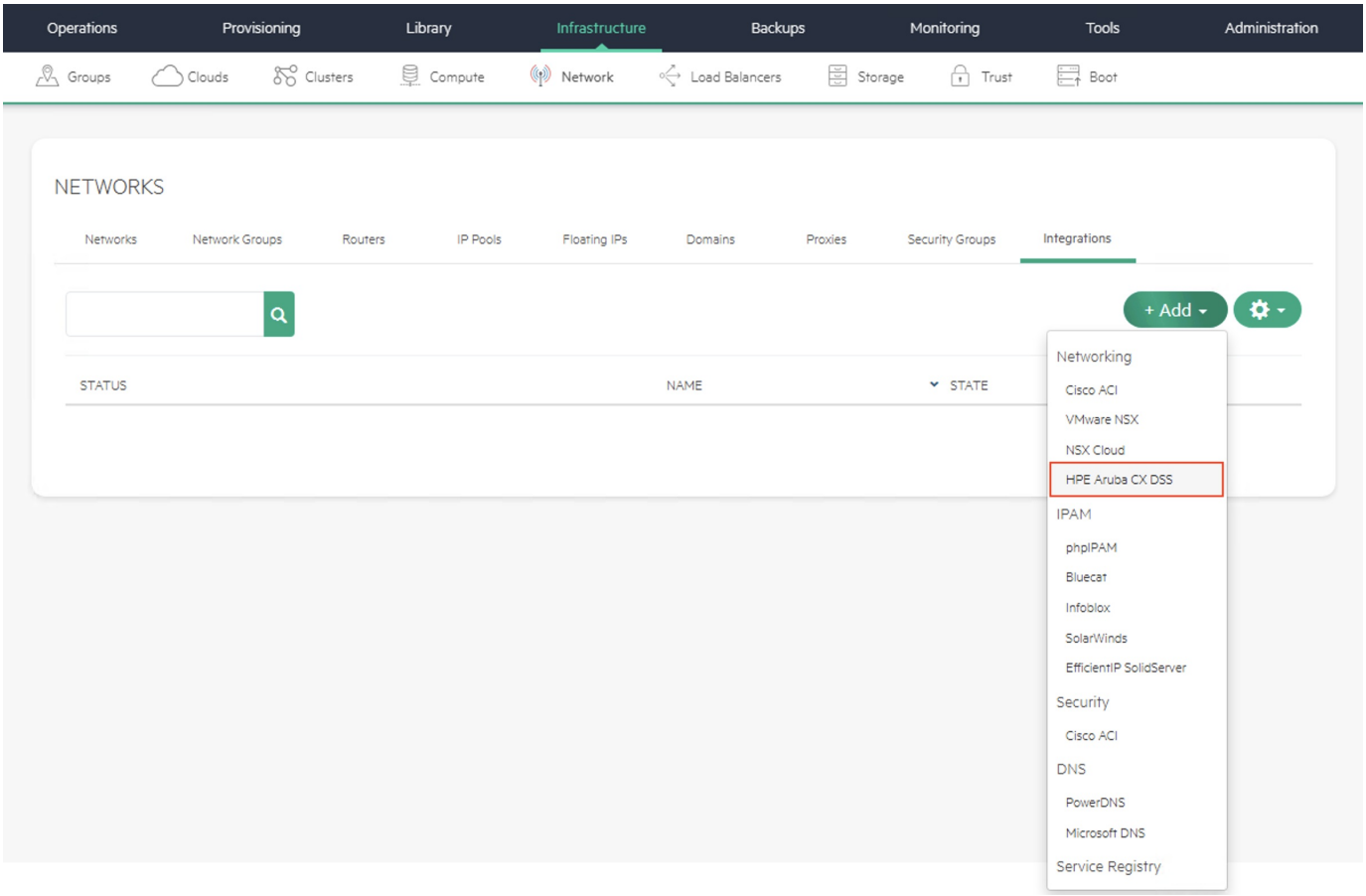
NOTE

- Download AFC and PSM from the **HPE Networking Support portal**
- For more information on deploying AFC and PSM, refer to the official documentation
- The AFC and PSM must have network connectivity to the CX 10000 switches
- Making full use of the VM Essentials Aruba CX 10000 integration requires credentials for AFC with API access granted and read/write access to AFC configuration

Adding *HPE Aruba CX DSS* Network Integration

Procedure

1. Navigate to Infrastructure > Network > Integrations
2. Select + Add > Networking > HPEAruba CX DSS



3. Enter the following details in the ADD NETWORK INTEGRATION form:

NAME

Name of the integration in VM Essentials

AFC ADDRESS

Enter the network address of the AFC

AFC USERNAME

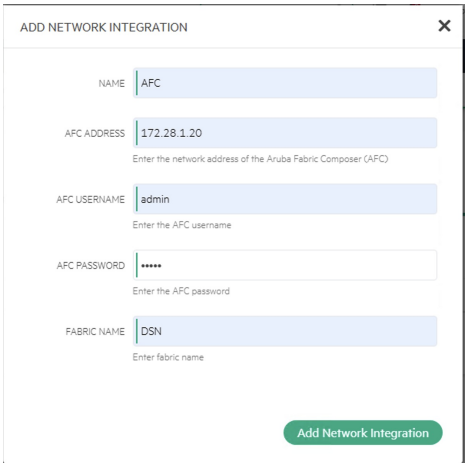
Enter the username

AFC PASSWORD

Enter the password

FABRIC NAME

Enter the fabric name from the AFC



4. Click Add Network Integration

Results

Upon add, the HPE Aruba CX DSS Network integration will be created.

> **NOTE**
> All fields can be edited after saving.

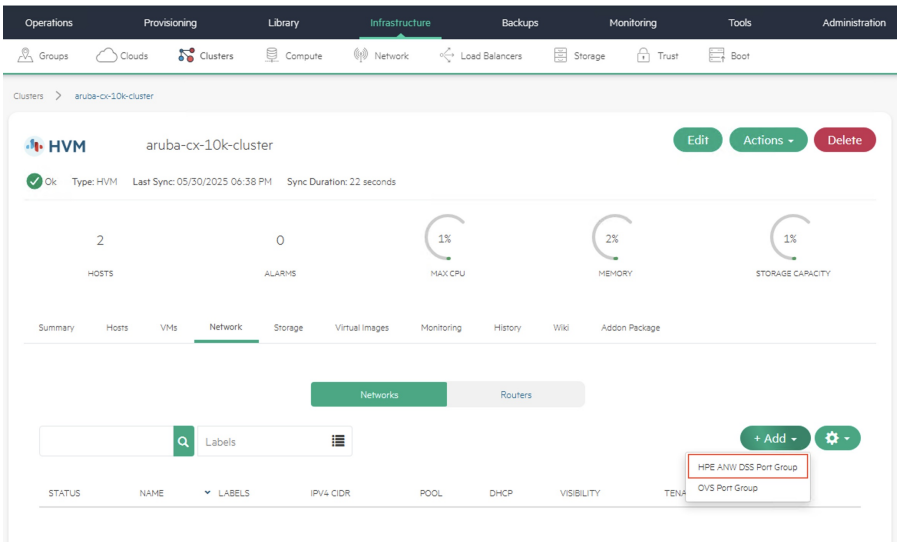
Create *HPE ANW DSS Port Group* Network

About this task

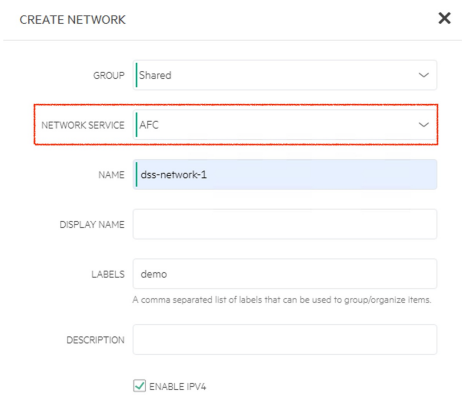
To create an HPE ANW DSS Port Group network, follow these steps:

Procedure

1. Navigate to Infrastructure > Network > Networks
2. Select + Add Network > HPE ANW DSS Port Group



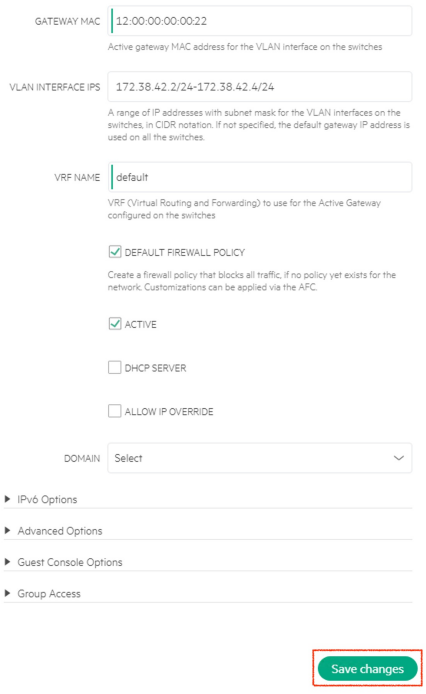
3. Select the Network Service in the CREATE NETWORK form:



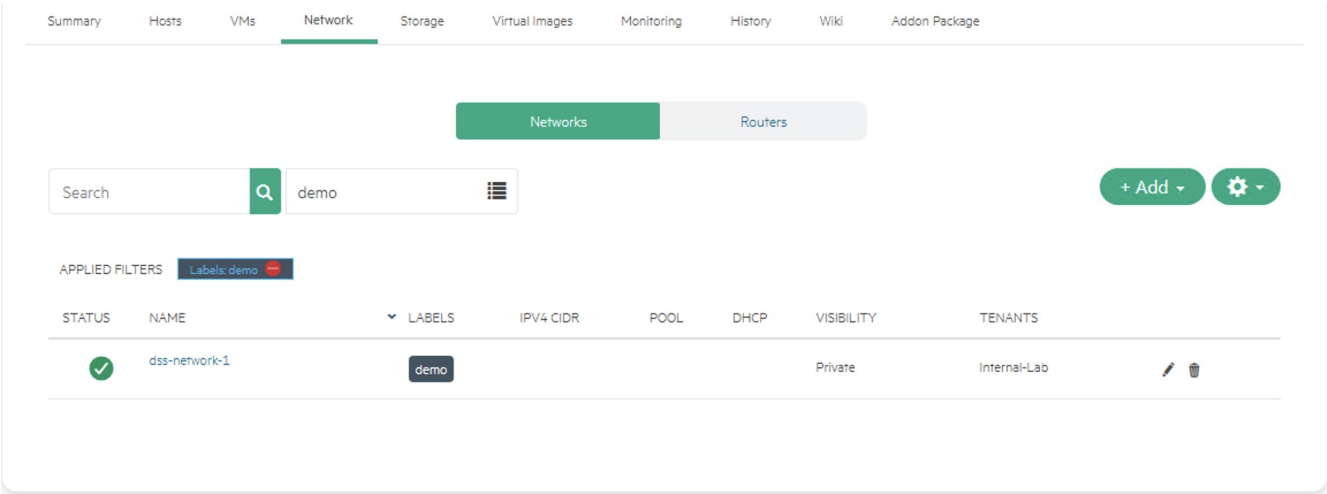
4. Enter the following details in the CREATE NETWORK form:

VLAN ID
4018
HOST PORT GROUP
bond0
The host network interface for which to enable microsegmentation
GATEWAY IP
172.38.42.1/24
IP address and subnet mask to act as the default gateway for the VLAN interface on the switches, in CIDR notation.
GATEWAY MAC
12:00:00:00:00:22
Active gateway MAC address for the VLAN interface on the switches
VLAN INTERFACE IPS
172.38.42.2/24-172.38.42.4/24
A range of IP addresses with subnet mask for the VLAN interfaces on the switches, in CIDR notation. If not specified, the default gateway IP address is used on all the switches.
VRF NAME
default
VRF (Virtual Routing and Forwarding) to use for the Active Gateway configured on the switches
DEFAULT FIREWALL POLICY
Create a firewall policy that blocks all traffic, if no policy yet exists for the network. Customizations can be applied via the AFC.
ACTIVE
DHCP SERVER
ALLOW IP OVERRIDE

5. Save the network by clicking on Save changes.


GATEWAY MAC
12:00:00:00:00:22
Active gateway MAC address for the VLAN interface on the switches
VLAN INTERFACE IPS
172.38.42.2/24-172.38.42.4/24
A range of IP addresses with subnet mask for the VLAN interfaces on the switches, in CIDR notation. If not specified, the default gateway IP address is used on all the switches.
VRF NAME
default
VRF (Virtual Routing and Forwarding) to use for the Active Gateway configured on the switches
DEFAULT FIREWALL POLICY
Create a firewall policy that blocks all traffic, if no policy yet exists for the network. Customizations can be applied via the AFC.
ACTIVE
DHCP SERVER
ALLOW IP OVERRIDE
DOMAIN
Select
IPv6 Options
Advanced Options
Guest Console Options
Group Access
Save changes

6. The network will be created and displayed in the list of networks.



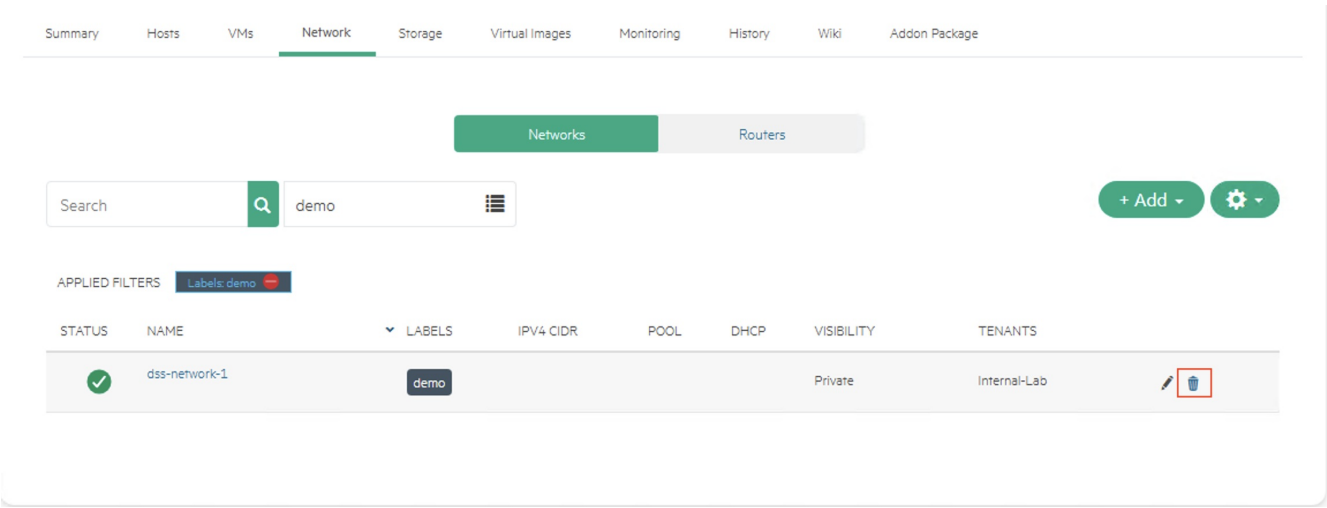
Delete *HPE ANW DSS Port Group* Network

About this task

To delete a HPE ANW DSS Port Group network, follow these steps:

Procedure

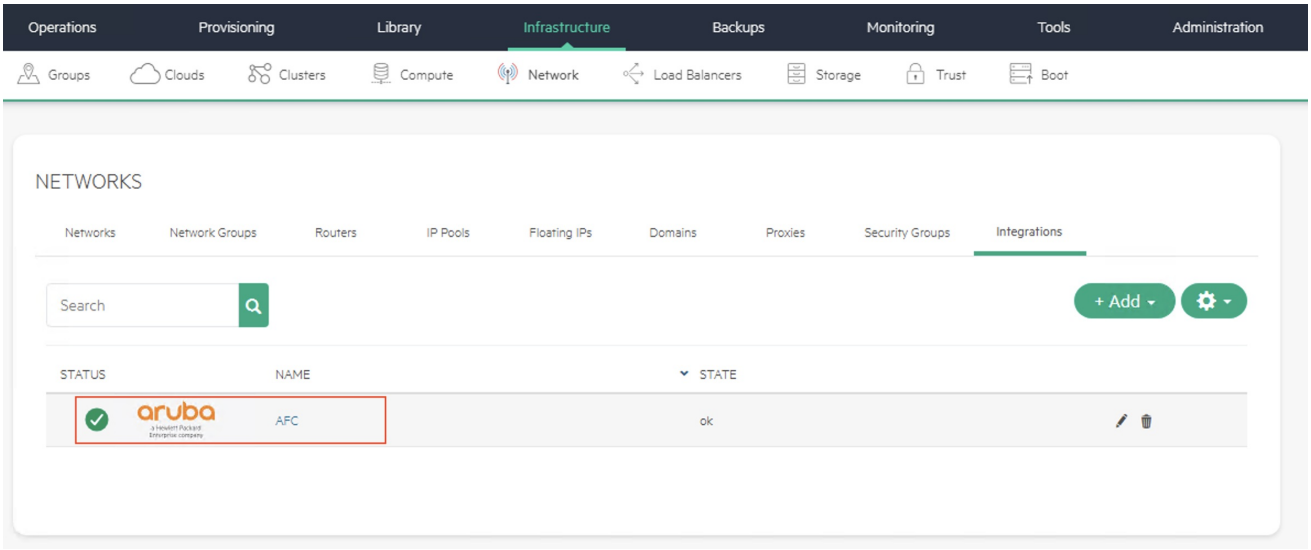
1. Navigate to
2. Select the network you want to delete from the list.
3. Click on the delete icon ( ) next to the network name.



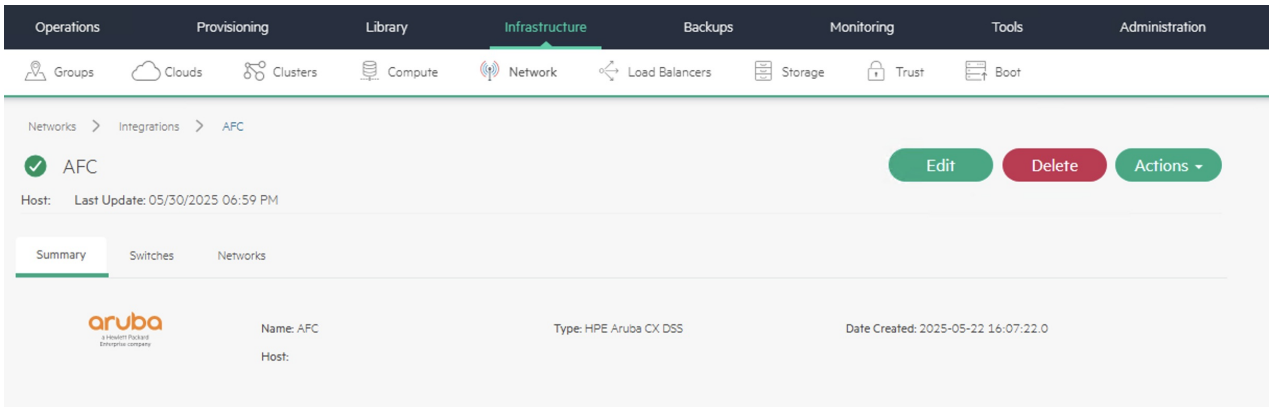
View *HPE Aruba CX DSS* Network Integration

To view the HPE Aruba CX DSS Network integration, follow these steps:

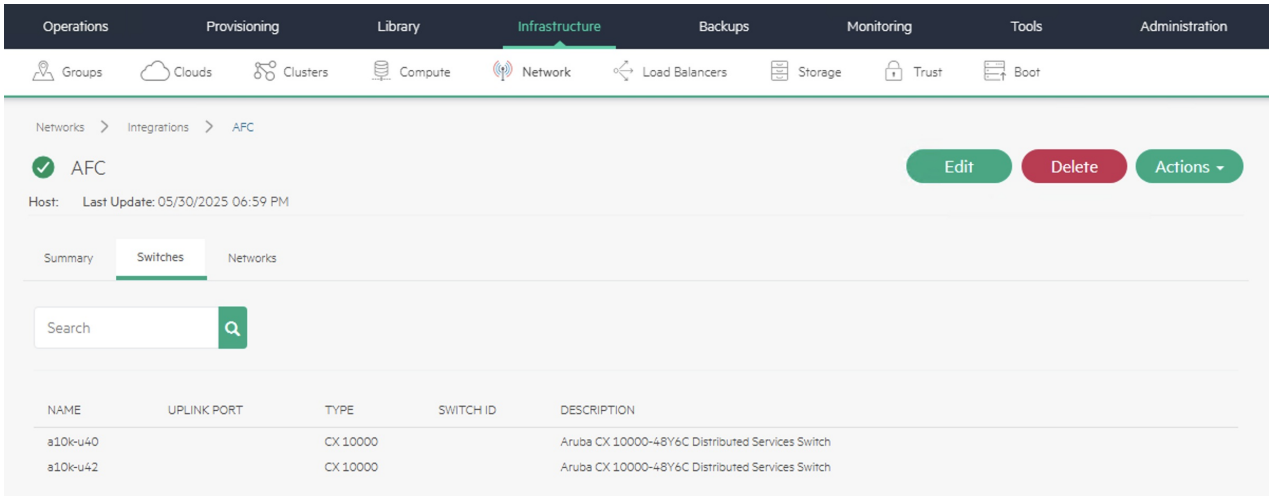
1. Navigate to Infrastructure > Network > Integrations
2. Select the HPE Aruba CX DSS integration from the list.



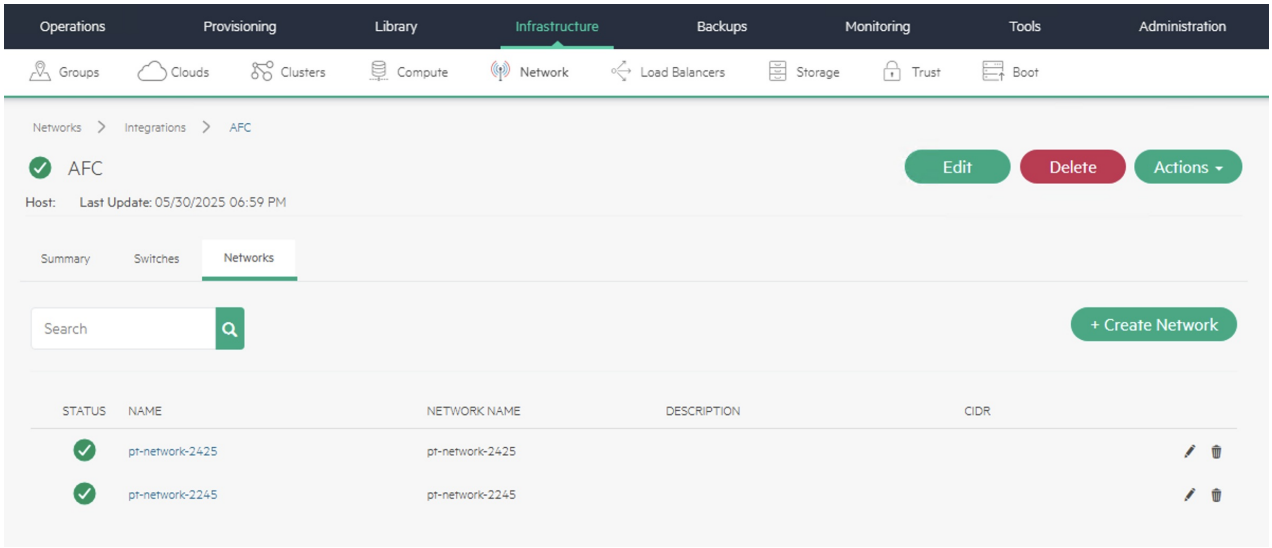
- **Summary** - Click on the Summary tab to view the summary of the integration.



- **Switches** - Click the Switches tab to view detailed information about all Aruba CX 10000 switches managed by the integration.



- **Networks** - Click on the Networks tab to view the networks associated with the integration.



Storage

Subtopics

- HPE Alletra MP Storage

HPE Alletra MP Storage

Subtopics

- Prerequisites
- Add HPE Alletra MP Storage
- Create Datastore
- Create Instance
- Add a storage server

Prerequisites

- All HPE Alletra MP Storage iSCSI ports are reachable from each of the cluster hosts
- The `multipath.conf` settings on each node should be configured as follows:

```
defaults {
   find_multipaths yes
   user_friendly_names no
}
```

Add HPE Alletra MP Storage

About this task

The first step is to create a storage server in VM Essentials. Once the storage server is added, you can create a datastore and provision Instances. Follow these steps to add a Storage Server:

Procedure

1. Navigate to Infrastructure > Storage
2. In the “Servers” tab, Click the + ADD button
3. From the ADD STORAGE SERVER wizard, input the following:

   NAME:

   Name of the storage server in VM Essentials

   TYPE:

   Select “HPE Alletra MP”

   URL:

   URL of HPE Alletra MP Storage (ex. `https://storage-system.example.com` or `https://192.1.2.3:1234`)

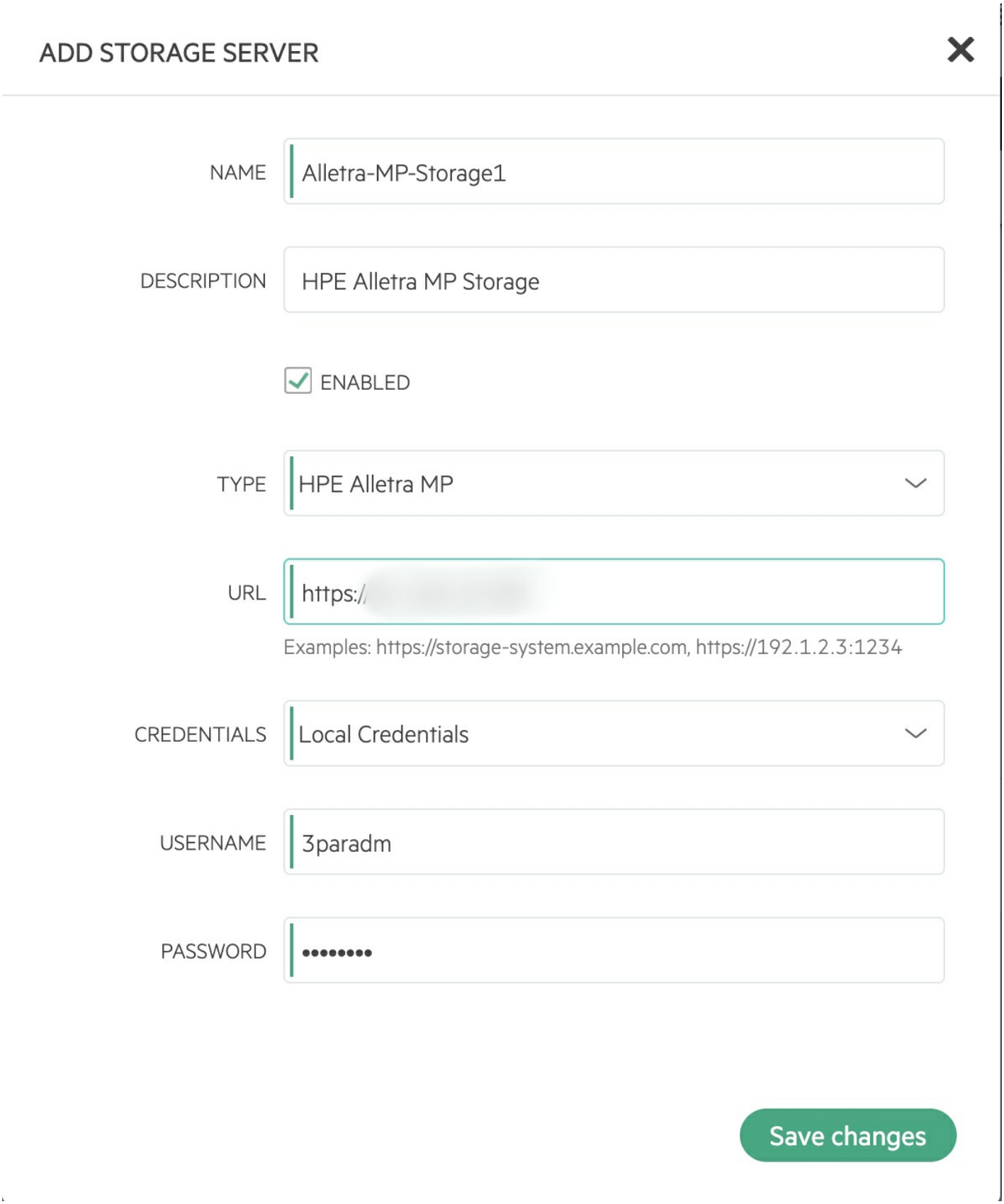
   USERNAME:

   Add your administrative user account

   PASSWORD:

   Add your administrative user account password
4. Select SAVE CHANGES

Results



The Storage Server will be added and displayed in the Datastore tab.

Create Datastore

About this task

Add a Datastore to the Storage Server.

Procedure

1. Navigate to Infrastructure > Clusters.
2. Click into the detail page for the cluster where the datastore is to be created.
3. Select the Storage tab.
4. Under the Data Stores sub tab, click + ADD.
5. From the ADD DATASTORE wizard, input the following:

   NAME:

   Name of the datastore in VM Essentials.

   TYPE:

   Select the type of storage system.

   STORAGE SERVER:

   Select the storage server that is created using the ADD STORAGE SERVER wizard.

   PROTOCOL TYPE:

   Select the type of storage protocol.

   RANSOMWARE DETECTION:

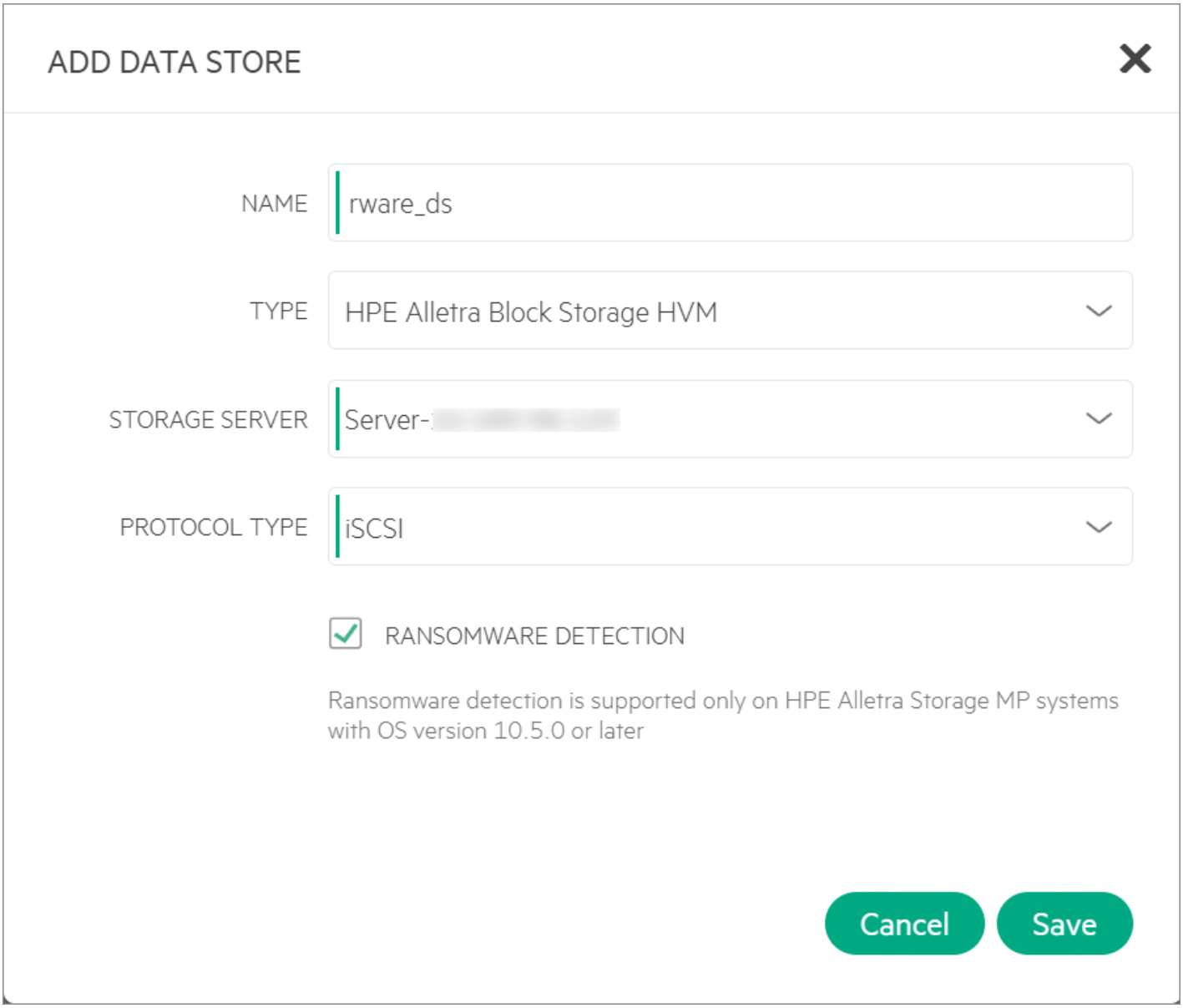
   Select the check box to enable ransomware detection for all VMs created with this datastore.

   NOTE

   The datastore creation fails if storage servers other than HPE Alletra Storage MP B10000 are selected along with the Ransomware Detection option.

6. Click SAVE.

Results



The datastore is added and displayed in the Datastore tab. Confirm that its status is healthy.

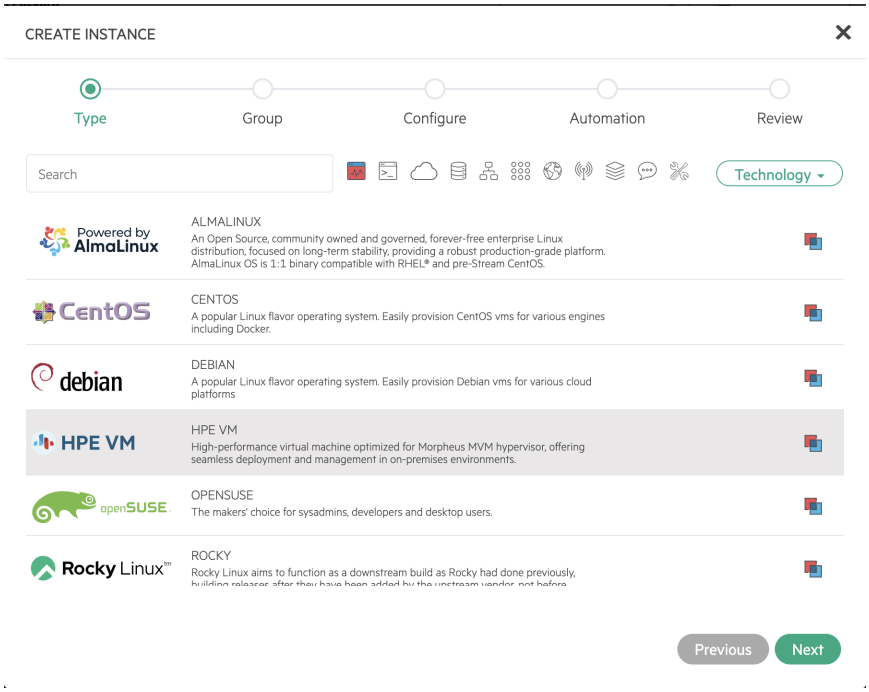
Create Instance

About this task

Create an Instance with the Datastore.

Procedure

1. Navigate to Provisioning > Instances
2. In the Instances tab, Click the + ADD button
3. From the ADD INSTANCE wizard input the following:
   - From the TYPE section: Select " HVM"
   - Click NEXT


CREATE INSTANCE
Type
Group
Configure
Automation
Review
Search
Technology
Powered by AlmaLinux
ALMALINUX
An Open Source, community owned and governed, forever-free enterprise Linux distribution, focused on long-term stability, providing a robust production-grade platform. AlmaLinux OS is 1:1 binary compatible with RHEL® and pre-Stream CentOS.
CentOS
CENTOS
A popular Linux flavor operating system. Easily provision CentOS vms for various engines including Docker.
debian
DEBIAN
A popular Linux flavor operating system. Easily provision Debian vms for various cloud platforms
HPE VM
HPE VM
High-performance virtual machine optimized for Morpheus MVM hypervisor, offering seamless deployment and management in on-premises environments.
openSUSE
OPENSUSE
The makers' choice for sysadmins, developers and desktop users.
Rocky Linux
ROCKY
Rocky Linux aims to function as a downstream build as Rocky had done previously,
Previous
Next

- From the GROUP tab, input the following:

  GROUP:

  Select the Group for the Instance

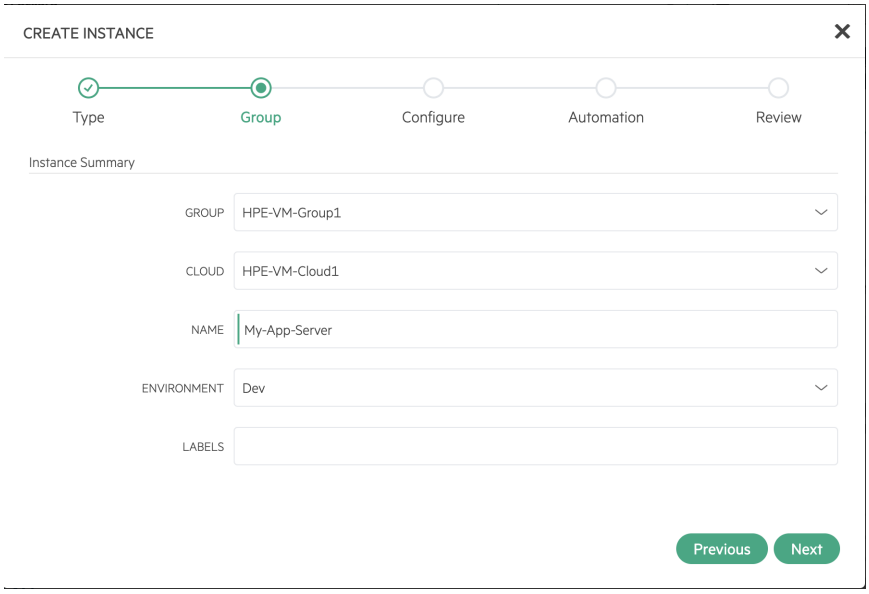
  CLOUD:

  Select the Cloud for the Instance

  NAME:

  Name for the Instance in VM Essentials

- Click NEXT



- From the CONFIGURE tab, input the following:

  LAYOUT:

  Select the Layout for the Instance

  PLAN:

Select the Plan for the Instance

RESOURCE POOL:

Select the Resource Pool (Cluster) for the Instance

VOLUMES:

Add one or more Volumes to the Instance. Select the datastore created in the previous section

NETWORK:

Add Networks to the Instance

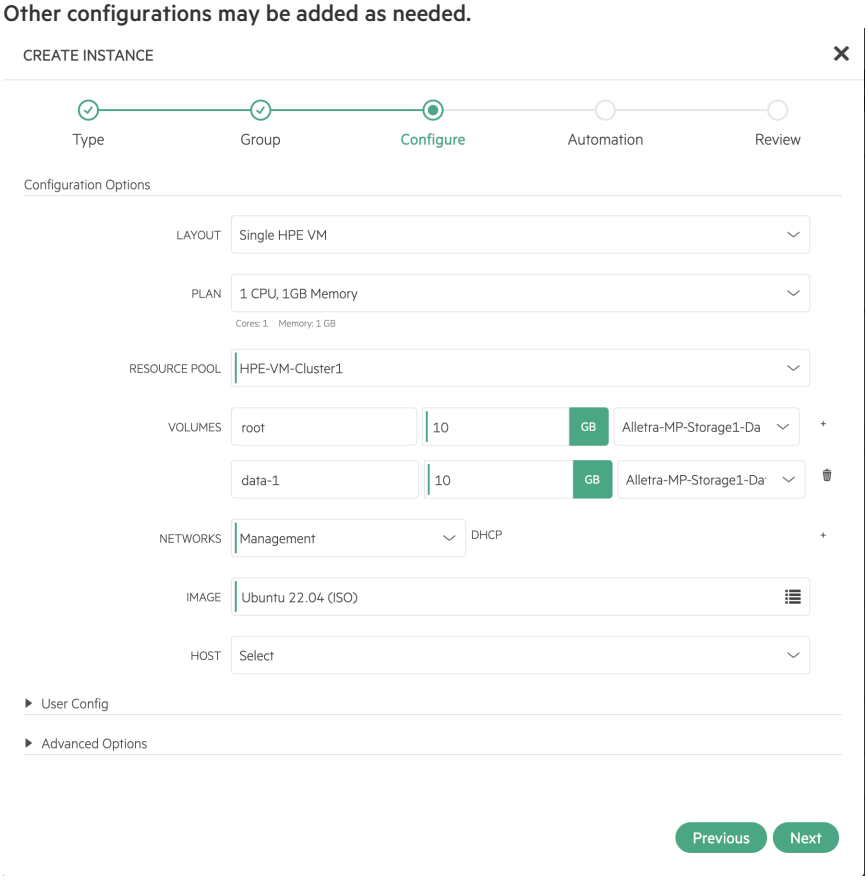
IMAGE:

Select the Image for the Instance

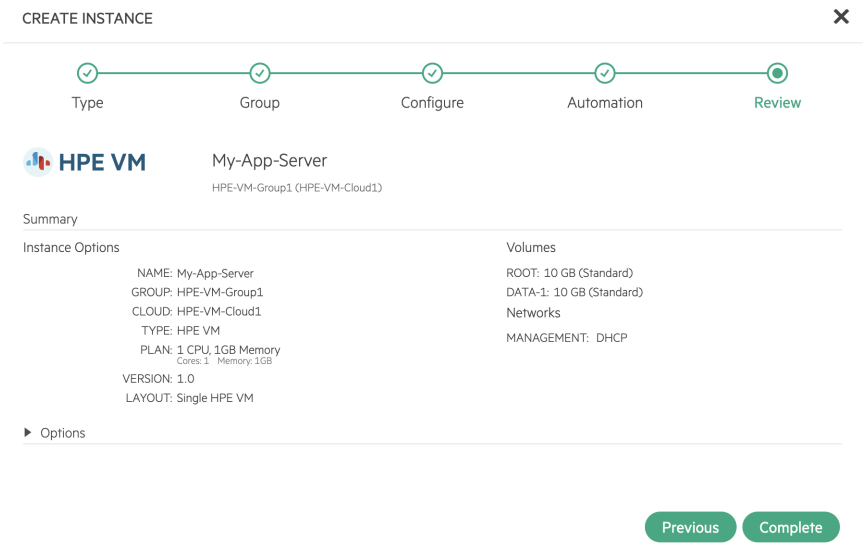
HOST:

Select the cluster host for the Instance

Other configurations may be added as needed.



- Click NEXT
- Add Automation Tasks, if needed
- Click NEXT
- Review the Instance configuration
- Click COMPLETE



Results

The Instance is now provisioned to the new datastore and is viewable within the Instances (Provisioning > Instances) section.

Add a storage server

The first step is to create a storage server in VM Essentials. After the storage server is added, you can view the storage summary, alerts, and pools. For more information on adding a storage server, see Add HPE Alletra MP Storage.

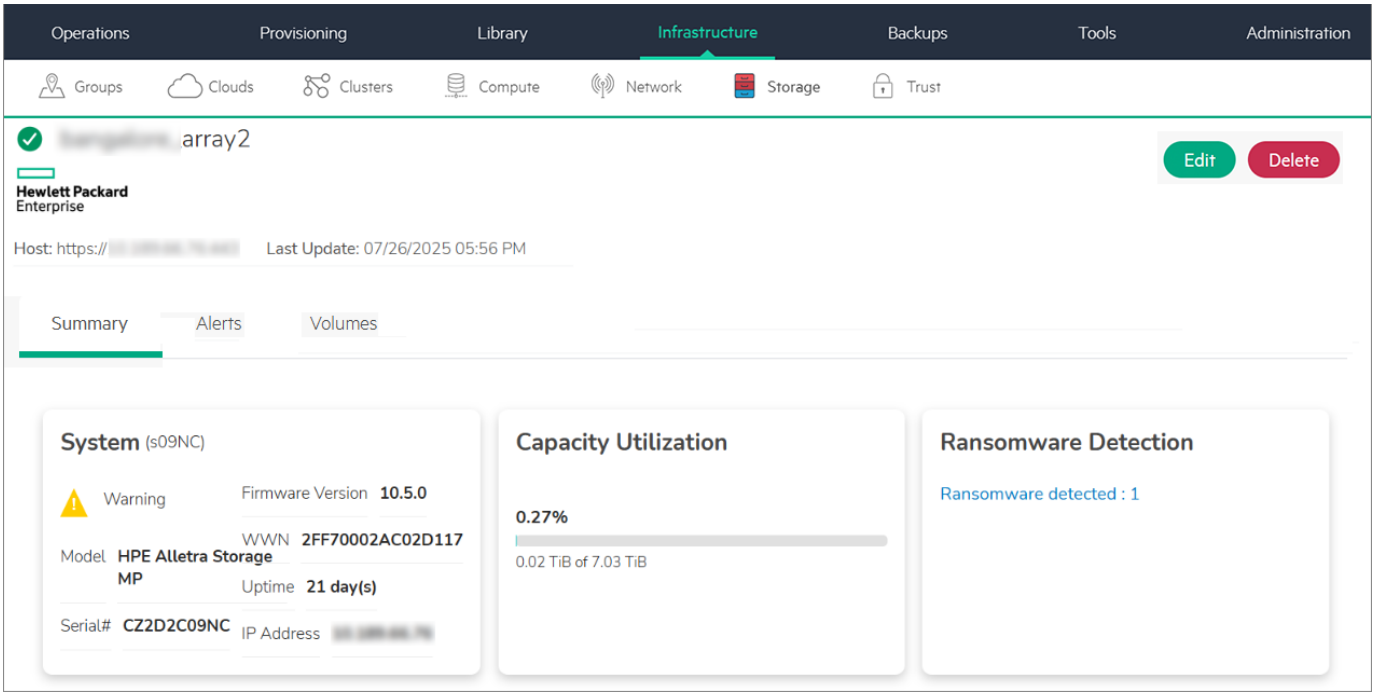
Subtopics

- Viewing the Summary page
- Viewing Alerts
- Viewing Volumes

Viewing the Summary page

The Summary tab displays system information, the capacity utilization of the system, and the number of ransomwares detected.

1. Navigate to Infrastructure > Storage > Servers.
2. In the Servers tab, select the server. The Summary tab displays the information for the selected server.



The Summary tab contains:

- **System**

  The following information is displayed in the System tile:

  - **Name:** Displays the system name of the selected server.
  - **Model:** Displays the model name of the system.
  - **Serial Number:** Displays the serial number of the system.
  - **Health status:** Displays the system health status of the array depending on the highest severity type of the alerts listed in the Alerts tab for the storage system. The health status values can be Critical, Normal, or Warning.

Highest Severity Type of Alerts	Health status
Critical or Fatal	Critical (The system has some major issues that will affect performance)
Major	Warning (The system is operational but with some non-critical issues)
Other types	Normal (The system is functioning as expected)

  - **Firmware version:** Displays the firmware version of the storage system.
  - **WWN:** Displays a unique identifier name of the system.
  - **Uptime:** Displays the total time that the system has been operational.
  - **IP Address:** Displays the IP address of the system.

- **Capacity Utilization**

  The Capacity Utilization tile displays the total and used capacity percentage of the selected storage system.

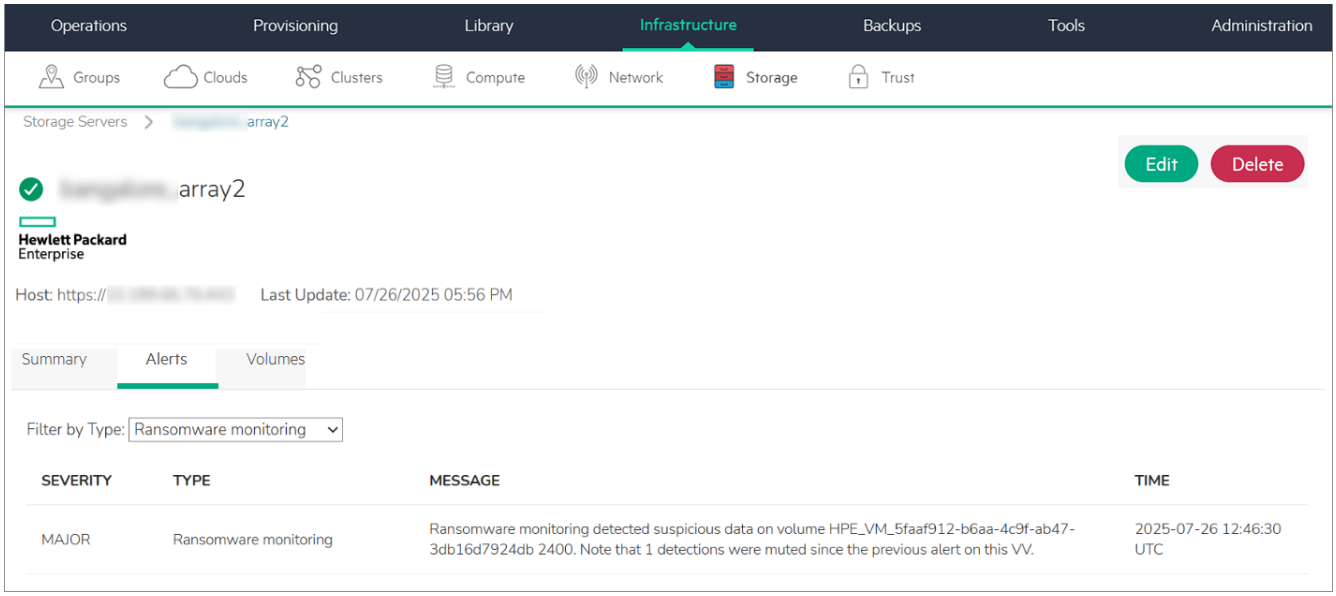
  - For models HPE Alletra MP B10000 and later, the Capacity Utilization tile populates the usable capacity.
  - For models prior to HPE Alletra MP B10000, the Capacity Utilization tile populates the raw capacity information.

> **NOTE**
>
> You can get the latest system information by clicking the Summary tab.

- **Ransomware Detection**

  The Ransomware Detection tile displays the number of ransomwares detected. A hyperlink is displayed when more than one ransomware alert is detected; otherwise, it is displayed as a plain text.

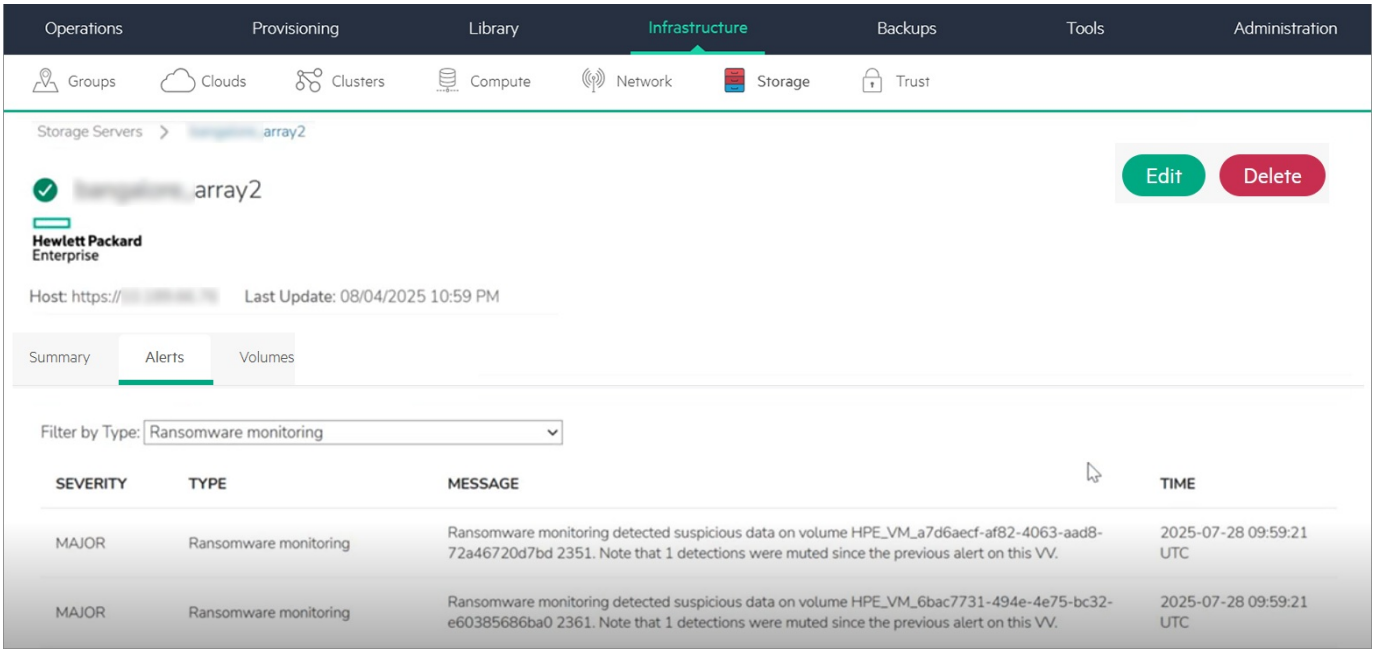
  On clicking the hyperlink, you can view the details of alert by selecting Ransomware monitoring as the Filter by Type.



Viewing Alerts

The Alerts tab displays system alerts with severity levels of Fatal, Critical, or Major.

1. Navigate to Infrastructure > Storage > Servers.
2. In the Servers tab, select the server.
3. Select the Alerts tab.
4. Select the type of alert that you want to view from the Filter by Type drop-down list.
5. The alerts displayed in the Alerts tab provide the following information:
   - **Severity:** Displays the severity of the alert. The severity can be Fatal, Critical, or Major. The severity of the alert determines the health status of the system.
   - **Type:** Displays the type of the alert message.
   - **Message:** Displays the description of the alert message.
   - **Time:** Displays the time when the alert was created. The UTC timezone is the standard timezone in the HPE Morpheus VM Essentials Software.



Viewing Volumes

The Volumes tab provides a list of all volumes, including their summary, capacity information, and ransomware monitoring status.

1. Navigate to Infrastructure > Storage > Servers.
2. In the Servers tab, select the server name.
3. Select the Volumes tab. You can view the following information:
   - **Name**: Displays the volume name for the VM.
   - **Details**: Displays the CD Drive volume or data disk associated with the VM name.
   - **Usage**: Displays a progress bar. The progress bar displays:
     - Used capacity in percentage.
     - Used capacity in either GiB or TiB, based on its value, in comparison to the total capacity.
   - **Ransomware Monitoring**: Indicates whether ransomware monitoring is enabled or disabled for the volume. Ransomware monitoring is enabled or disabled while creating the datastore.

     NOTE

     Once ransomware monitoring is enabled for a datastore, the ransomware monitoring status cannot be edited.

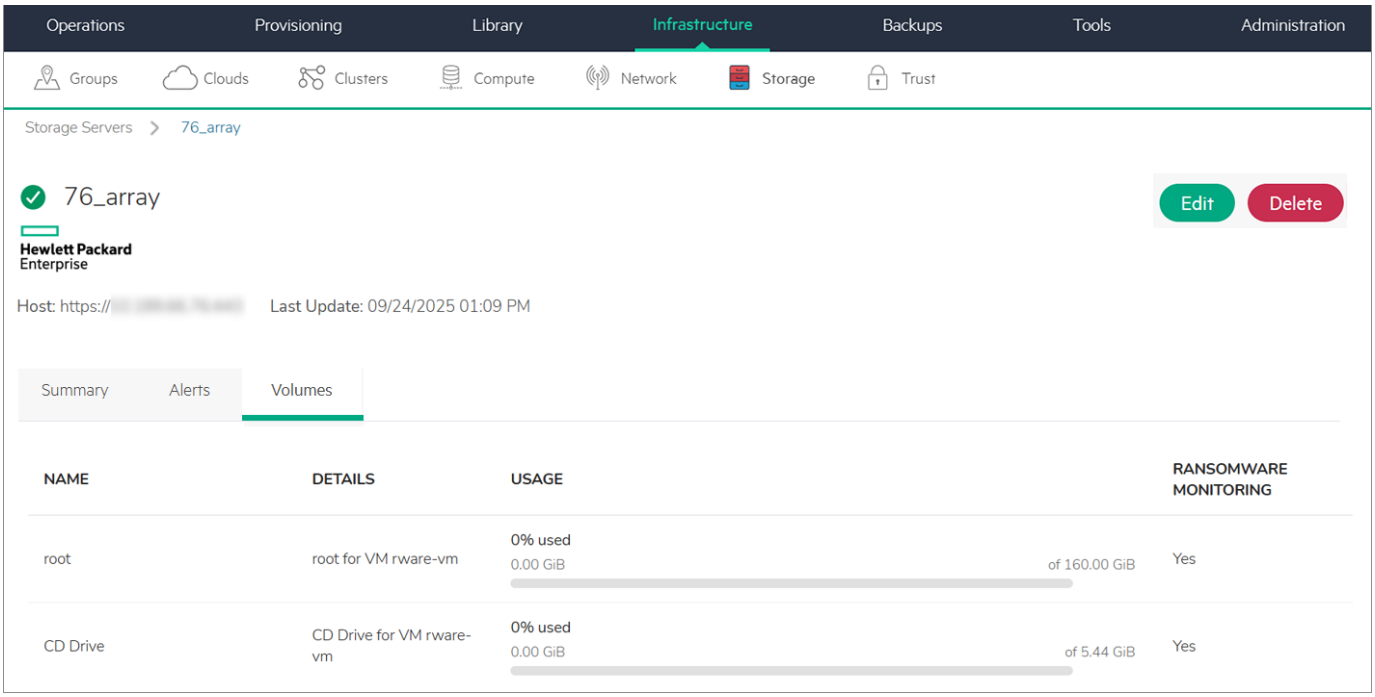


Image preparation

Subtopics

- Image Prep (Windows)
- Creating a Windows Image
- Creating a VM Essentials VMware Image
- Creating a CentOS/RHEL 7 Image
- Creating a CentOS/RHEL 8 Image

Image Prep (Windows)

This section will go through the steps to prepare a Windows image which can be successfully provisioned to HVM clusters. Additionally, this image can serve as a template from which additional images and VM Essentials Library items can be built. In this example case, we'll start from downloading a Windows Server 2019 ISO directly from the Microsoft download center and go all the way through to creating a new Instance Type in VM Essentials that users can provision on-demand.

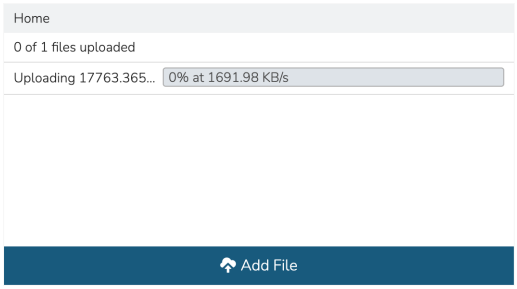
With the Windows ISO already downloaded, begin by uploading the ISO as a Virtual Image in VM Essentials. Virtual Images are added in Library > Virtual Images. Click + ADD and then choose "ISO." Before adding the file itself, set the following configurations on the Virtual Image:

- **NAME:** A name for the Virtual Image in VM Essentials, such as "Windows Server 2019 ISO"
- **OPERATING SYSTEM:** "windows server 2019"
- **MINIMUM MEMORY:** Filters out Service Plans at provision time which do not meet the minimum value. For this image type, I've set 4 GB

In addition to the above, there are a number of checkbox configurations here (many of them are in the expandable "Advanced" section), some of which are checked by default. They should all be unchecked except for "VIRTIO DRIVERS LOADED?" within the "Advanced" expandable section.

With the configurations set, it's time to upload the ISO to VM Essentials. Keep in mind that if you do not specify a bucket in which the file should be uploaded, it will be uploaded to the appliance itself. If you choose to do this, be sure you have enough space to store the images you need. Within the UPLOAD VIRTUAL IMAGE modal is a large dropzone labeled "Drop Files Here." You can drag and drop the ISO file here or you can click the button labeled "Add File" and browse for it. A progress bar will appear, wait until the file is completely uploaded before

you save and dismiss the modal. After the file has completely uploaded, click SAVE CHANGES.

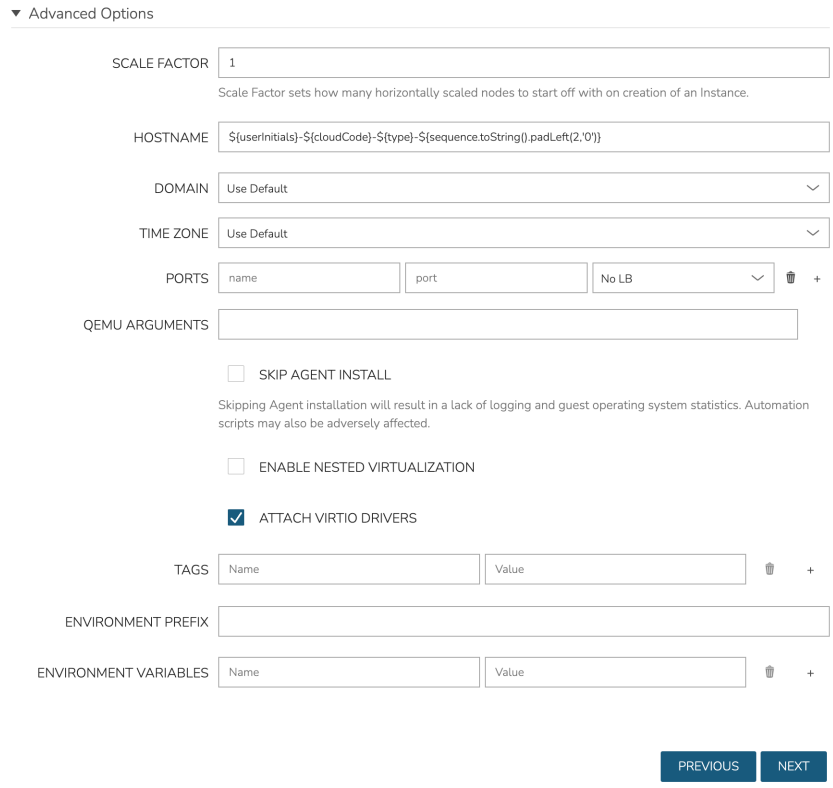


Next, we'll provision a VM from the ISO using the built-in HVM Instance Type. Once running, we will configure the VM to any specific requirements and convert it to a template. Navigate to Provisioning > Instances and click + ADD. On the TYPE tab of the Instance provisioning wizard, we select the Instance Type to provision. In this case, select "HVM" and click NEXT.

On the GROUP tab, select the Group and Cloud containing the target MVM Cluster and provide a name for the new Instance. In my case, I have an automatic naming policy setting my Instance name, but depending on your appliance configuration you may need to enter a custom name. Click NEXT.

On the CONFIGURE tab, first select the IMAGE. Select the Windows server ISO that was uploaded in the previous step. Based on the minimum memory configuration that was set on the Virtual Image, Plans which are too small will be filtered out. Among compatible Plans, select one that meets your requirements. Next, set the RESOURCE POOL, which is the HVM cluster you're targeting. Configure disks and disk sizes, as well as network details (this will vary based on HVM cluster configuration). Finally, select the HOST, which is the HVM host within the cluster that the new Instance should initially be provisioned onto.

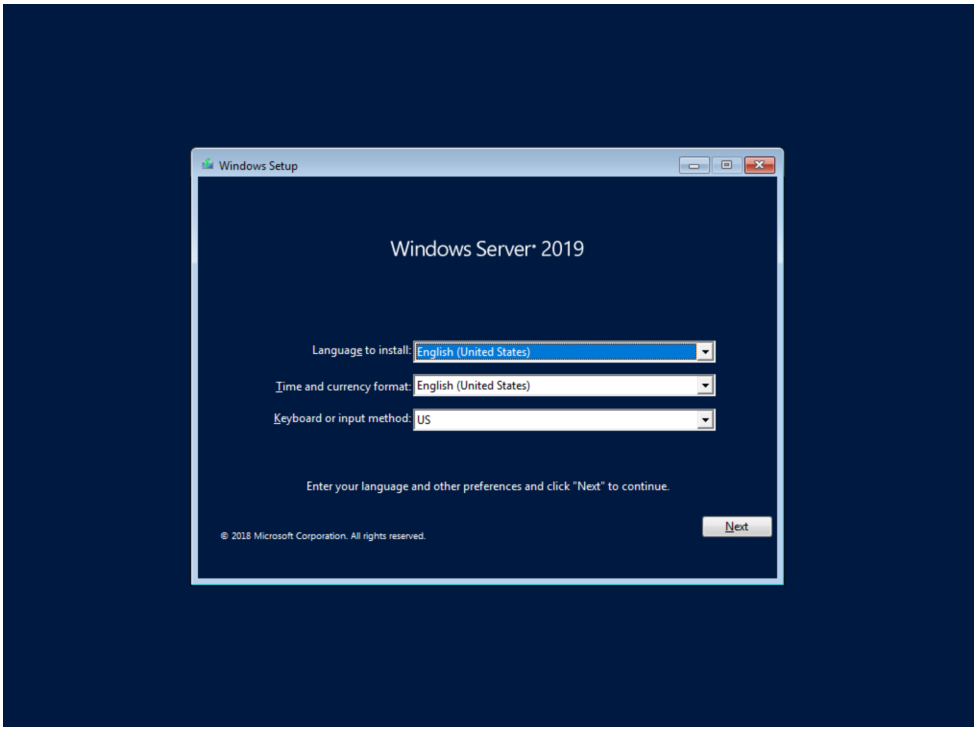
As a final step, we need to also expand the "Advanced Options" section and make sure "ATTACH VIRTIO DRIVERS" is checked. This will attach an ISO containing the VirtIO drivers which we'll use later. Click NEXT.



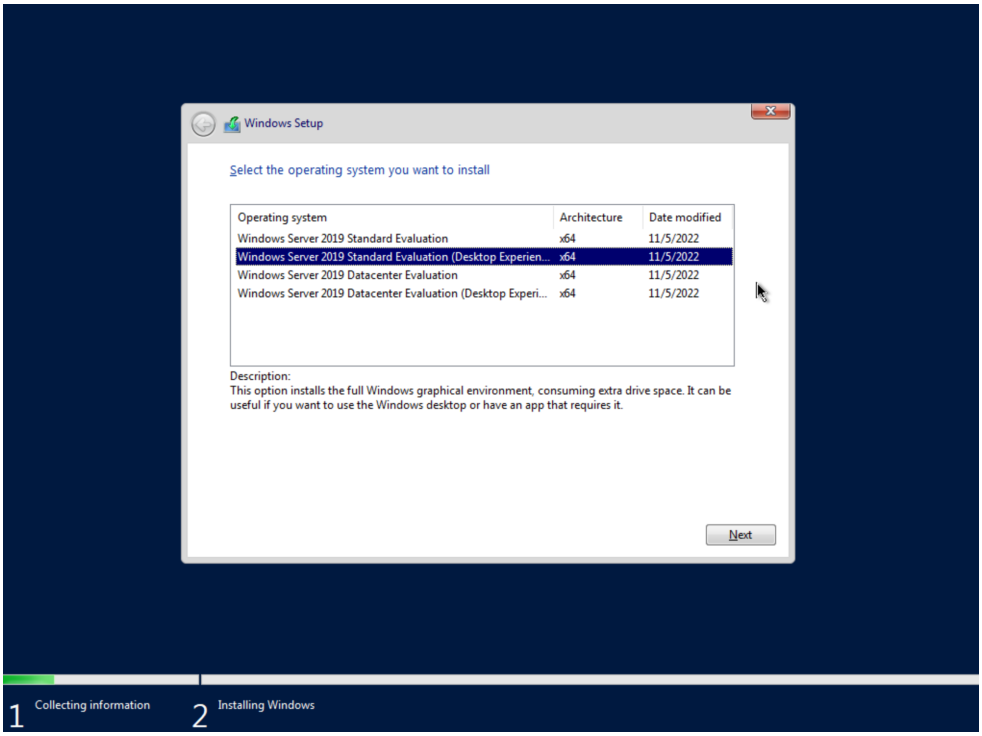
The final two tabs of the wizard, AUTOMATION and REVIEW, do not require any configuration changes though you may want to review the Instance settings on the final tab. When done, click COMPLETE.

Click on the newly provisioning Instance from the Instances list page. Since this image is being provisioned for the first time, the image must be uploaded to the HVM host. This can take a little bit of time but any future attempts to provision workloads from this image will skip this step. Wait for the Instance to fully complete and appear in a green "Ready" status.

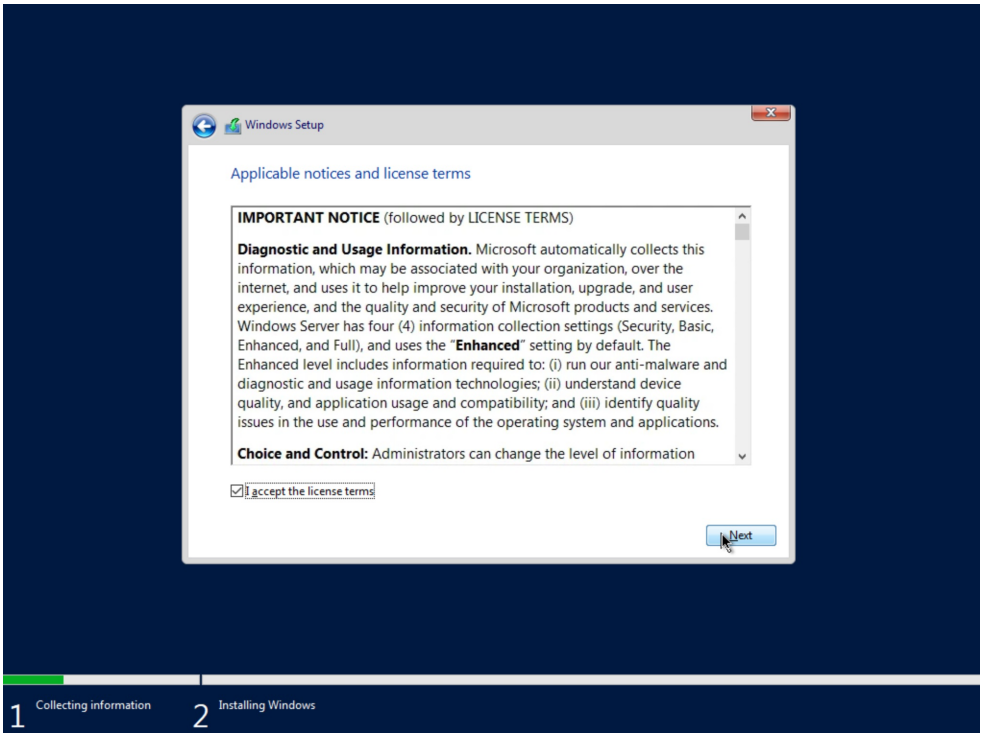
Once the Instance has fully finished provisioning, launch a console session by clicking ACTIONS and then "Open Console." This will open a new window with a console session into the VM.


Windows Setup
Windows Server 2019
Language to install: English (United States)
Time and currency format: English (United States)
Keyboard or input method: US
Enter your language and other preferences and click "Next" to continue.
© 2018 Microsoft Corporation. All rights reserved.
Next

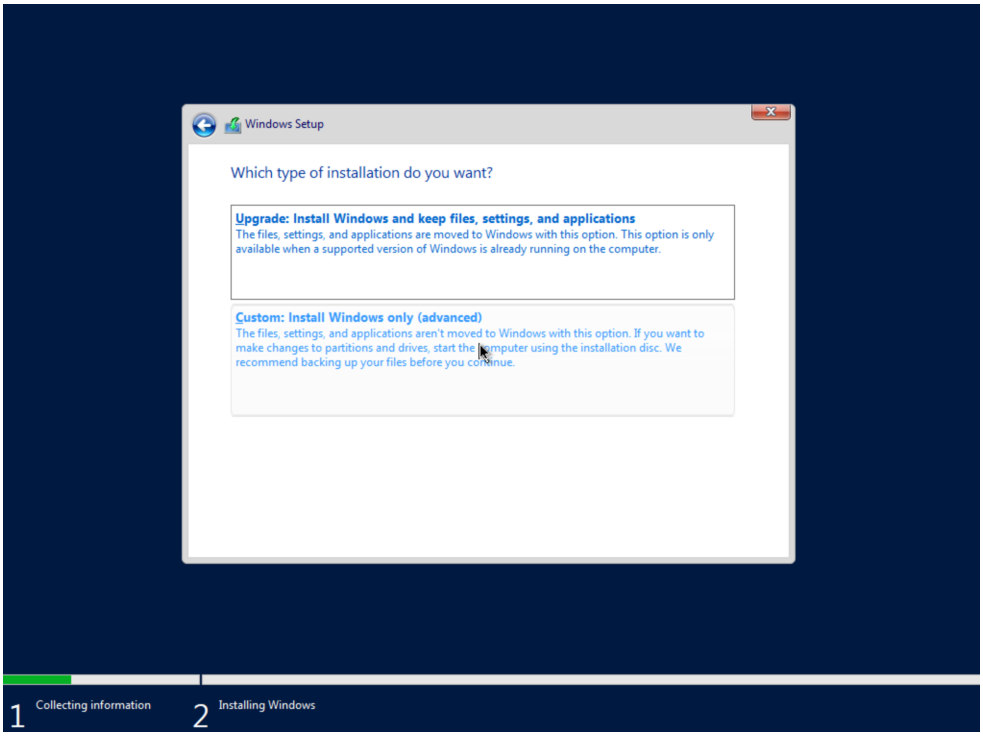
After selecting the language, click “Next.” On the following screen, click “Install Now.” This will begin the Windows setup process on our new VM. You’ll next select the operating system type you wish to install. For this example, I’m installing 2019 standard with desktop experience. Click “Next.”



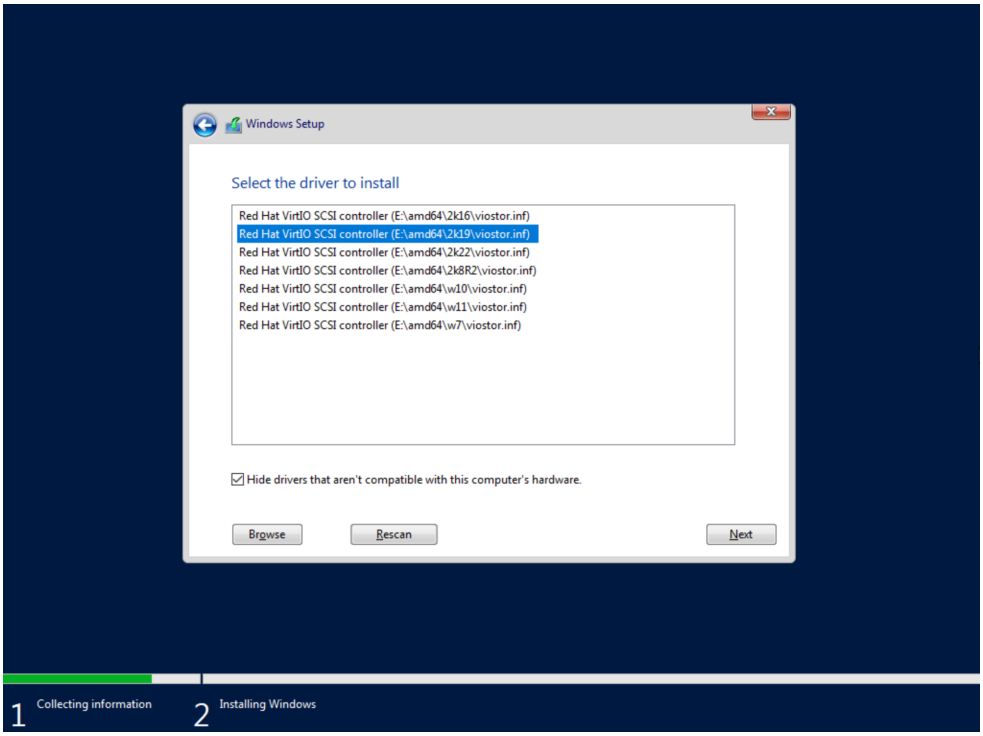
Accept the licensing terms and click “Next.”


Windows Setup
Applicable notices and license terms
IMPORTANT NOTICE (followed by LICENSE TERMS)
Diagnostic and Usage Information. Microsoft automatically collects this information, which may be associated with your organization, over the internet, and uses it to help improve your installation, upgrade, and user experience, and the quality and security of Microsoft products and services. Windows Server has four (4) information collection settings (Security, Basic, Enhanced, and Full), and uses the "Enhanced" setting by default. The Enhanced level includes information required to: (i) run our anti-malware and diagnostic and usage information technologies; (ii) understand device quality, and application usage and compatibility; and (iii) identify quality issues in the use and performance of the operating system and applications.
Choice and Control: Administrators can change the level of information
I accept the license terms
Next
1 Collecting information
2 Installing Windows

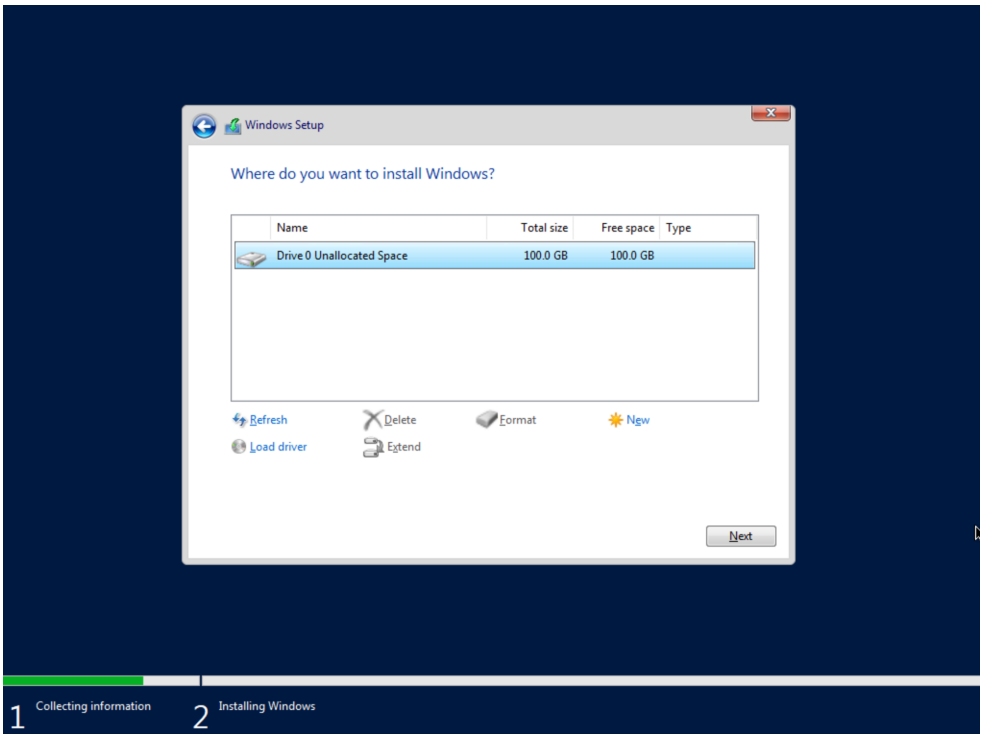
On the next screen, choose a custom install.


Windows Setup
Which type of installation do you want?
Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.
Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.
1 Collecting information
2 Installing Windows

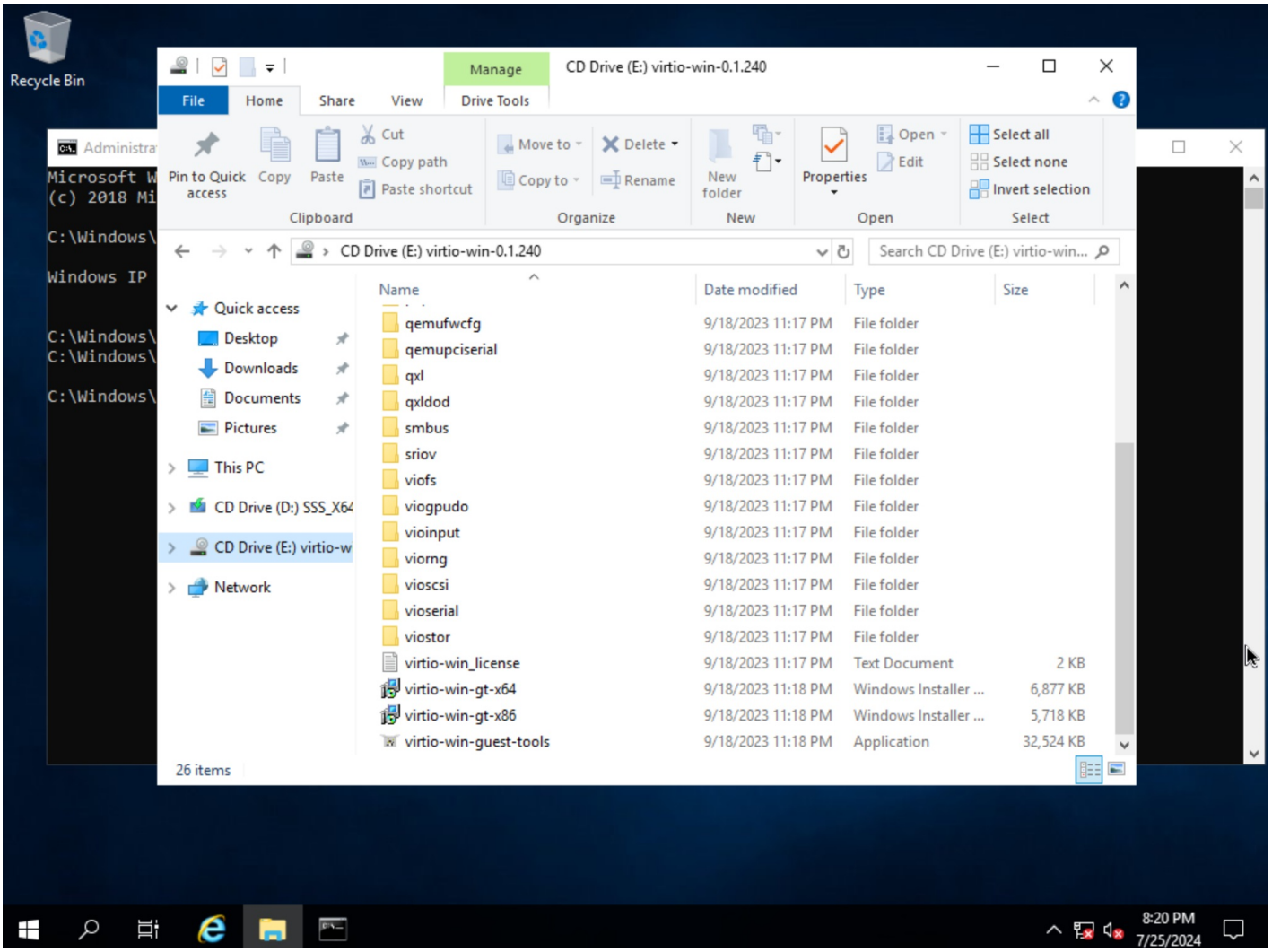
The next screen asks where Windows should be installed and may be empty. Click “Load Driver” to locate the mounted disk image containing the VirtIO drivers. The search should return a number of VirtIO SCSI controller packages for various Windows flavors. Select the proper package for the Windows version being installed. Click “Next.”


Windows Setup
Select the driver to install
Red Hat VirtIO SCSI controller (E:\amd64\2k16\viostor.inf)
Red Hat VirtIO SCSI controller (E:\amd64\2k19\viostor.inf)
Red Hat VirtIO SCSI controller (E:\amd64\2k22\viostor.inf)
Red Hat VirtIO SCSI controller (E:\amd64\2k8R2\viostor.inf)
Red Hat VirtIO SCSI controller (E:\amd64\w10\viostor.inf)
Red Hat VirtIO SCSI controller (E:\amd64\w11\viostor.inf)
Red Hat VirtIO SCSI controller (E:\amd64\w7\viostor.inf)
Hide drivers that aren't compatible with this computer's hardware.
Browse
Rescan
Next
1 Collecting information
2 Installing Windows

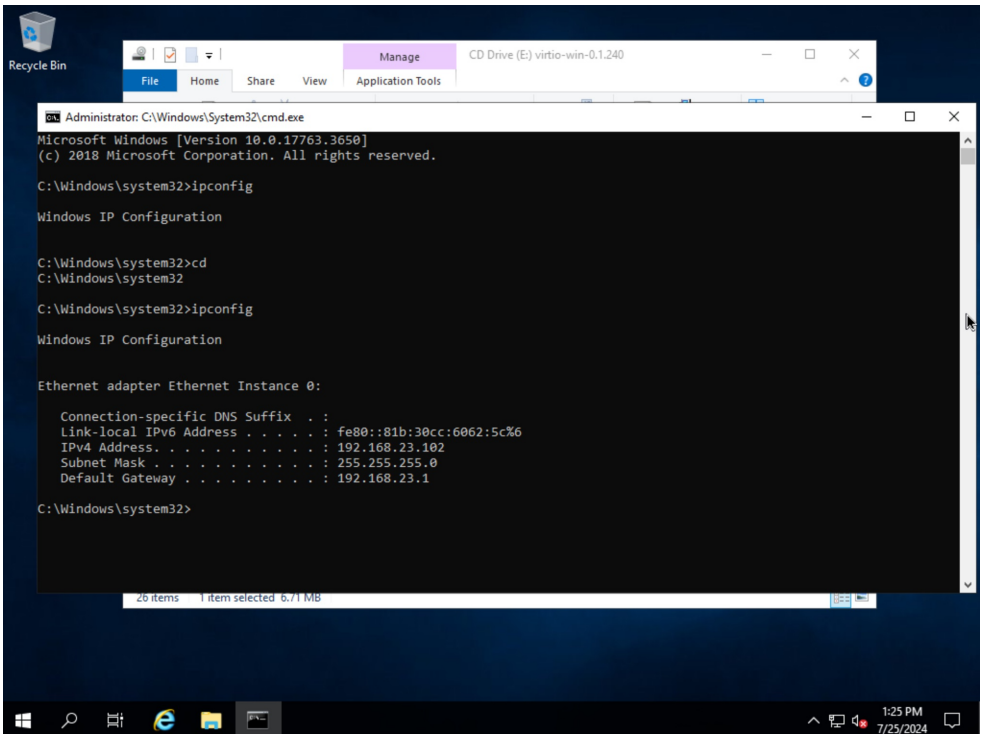
After a moment, we're back at the screen asking where Windows should be installed. We should see the disk(s) of size and type selected at the time the VM was provisioned. Select the proper disk and click "Next." The Windows installation will now begin. Once Windows has fully installed, proceed to the next step.



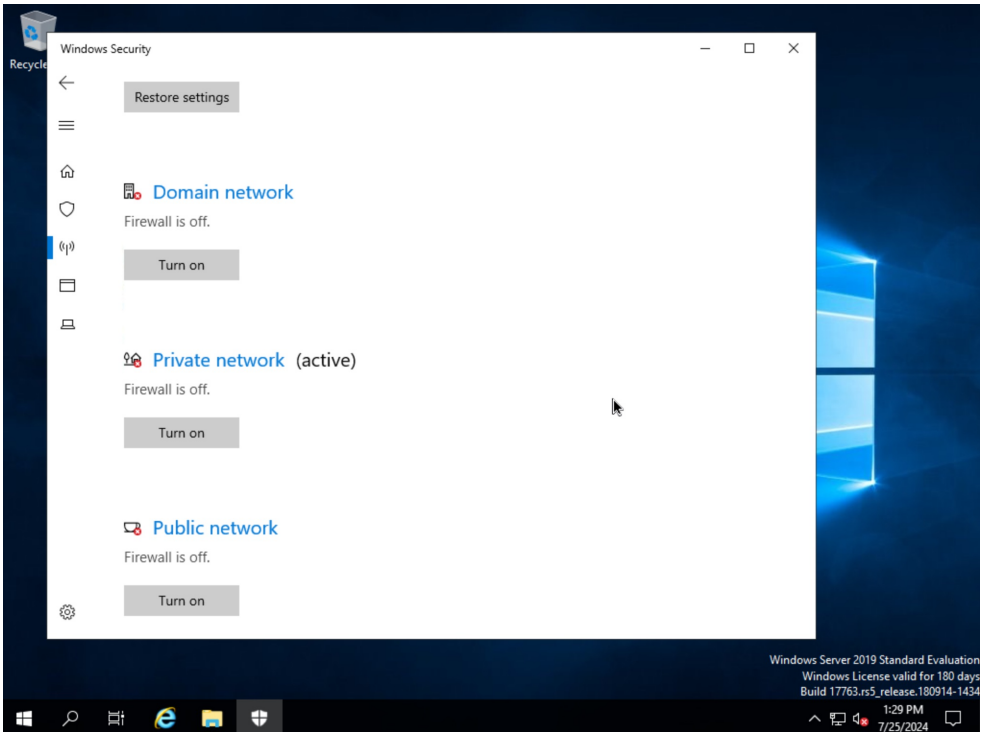
Following installation, Windows will restart and prompt for an Administrator user password. Set the password and log in as Administrator. Currently, there are no network interfaces configured. We need to install the VirtIO drivers to get this machine onto the network. We have a disk image mounted with the driver installer so we need to navigate to that drive and launch the installer. Open Windows Explorer and locate the drive in the side bar. In my case, it's the E: drive. Right-click on `virtio-win-guest-tools` and select "Install."



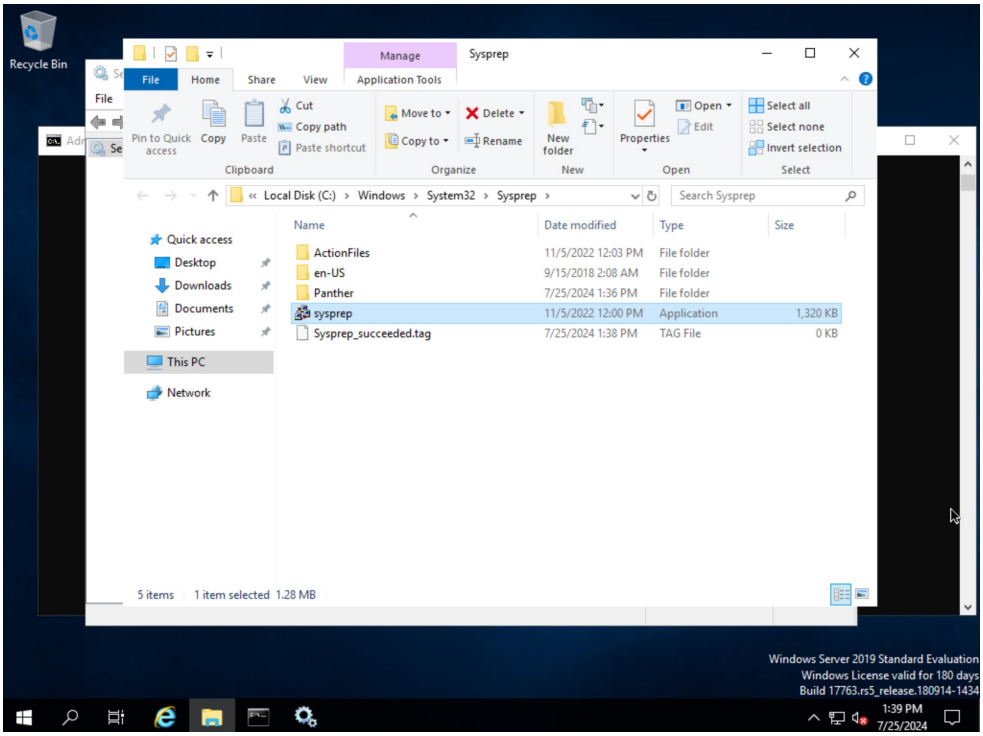
Step through the installer. Simply click “Next” or “Install” through each step, there are no configuration changes needed. Once the installer has completed, click “Finish.” You can confirm we now have a network interface by opening a Command Prompt session and using the `ipconfig` command. One network adapter should be listed.



We can now eject the two virtual disks, drives D: and E: in my case. Then, launch Windows Security so we can disable firewalls. Turn off firewall for domain, private network, and public network.



Next, back in Command Prompt, run `winrm quickconfig` to configure `winrm`. Within `Services`, ensure that `winrm` (Windows Remote Management) is set to automatic on startup. Right-click on the Start button and select Run. Enter “sysprep” and click OK. In the Windows Explorer window that appears, right-click on `sysprep` and click “Run as Administrator”. Under “Shutdown Options”, choose Quit and click OK. If this is set to shutdown, VM Essentials will simply restart the VM. Once this is completed, a new file `Sysprep_succeeded.tag` appears in Windows Explorer.



We’re now done configuring Windows and the console window can be closed. We’ll move on to creating a template from the VM we just configured. Begin by opening an SSH session into the VM Essentials appliance server. Confirm `jq` is up to date on the appliance box (`apt install jq`). Then, go ahead and stop the running Windows VM. We can do this from the Instance detail page in VM Essentials. Click ACTIONS and then “Stop Server.” Still on the Instance detail page, click ACTIONS and then “Import as Image.” This will perform a snapshot and create a new Virtual Image (Library > Virtual Images).

The Virtual Image is not usable until it’s in an active status and the UI indication may display an active status even before it’s fully ready. If it’s “SAVING” or “QUEUED,” it is still being prepared and saved. To determine the current status of the Virtual Image, check with a call to VM Essentials API like the one below. When the return output lists a status of “Active,” the image is ready to be provisioned from.

```
curl -k --request GET --url https://xx.xx.xx.xx/api/virtual-images/<id>
--header 'accept: application/json' --header 'authorization: Bearer xxx-xxx-xxx-xxx-
```

```
xxx' |
jq '.virtualImage.status'
```

Once saved, additional configurations are needed on the Virtual Image in VM Essentials. Edit the new Virtual Image and check the following configurations:

- **MINIMUM MEMORY:** Set as appropriate
- **SYSPREPPED/GENERALIZED IMAGE?:** Checked
- **INSTALL AGENT?:** Checked
- **USERNAME:** Remove if present
- **PASSWORD:** Remove if present
- **VIRTIO DRIVERS LOADED?:** Checked

All other checkbox-type configurations not mentioned in the above list should be unchecked. Click SAVE CHANGES.

At this point all image preparation steps are completed. Repeat the process of provisioning an HVM Instance Type selecting the new image in the future when needed.

Creating a Windows Image

Subtopics

Supported Versions
Image Preparation

Supported Versions

2008R2, 2012, 2012R2, 2016, 2019, 2022

Image Preparation

About this task

Create a new machine in VMware vCenter and install a base version of your preferred Windows build. The smaller the VMDK drive, typically the faster you can clone and deploy. Utilizing VM Essentials, provisioning and post deploy scripts can expand drives to desired sizing.

Procedure

1. Ensure VMware Tools is installed on the operating system.
2. Apply any service packs / updates to the operating system.
3. Configure WinRM to allow remote management and open the firewall. This is optional if using VMware Tools RPC mode for agent install and VM Essentials Agent for guest exec. To enable this, under local computer Administrator, open a command prompt and run

   ```
   winrm quickconfig
   ```

4. Install .Net at least 4.5.2
5. Ensure Windows Firewall will allow WinRM connections.
6. Shutdown the virtual machine and convert to a template.

Results

NOTE

WinRM is not required and is used as a fallback when using vmtools guest exec and customizations

NOTE

Morpheus will sysprep images based on the “Force Guest Customizations” flag under the Virtual Image’s settings when using DHCP. Ensure a sysprep has not been performed on the template if this flag is enabled or if using Static IPs/IP Pools when provisioning, which will always use Guest Customizations and trigger a sysprep.

IMPORTANT

VM Essentials supports the use of SR-IOV network adapters with VMware Clouds. Windows images must have SR-IOV network drivers installed to work with this adapter type. If they do not, provisioning will fail.

Creating a VM Essentials VMware Image

VM Essentials comes out of the box with a default set of blueprints for use in many modern deployment scenarios. These consist mostly of base operating system images with a few additional adjustments. These adjustments typically include the addition of cloud-init (which is highly recommended to be used in most environments, but not mandatory). However, in many on-premise deployments there are custom image requirements as well as networking requirements. This guide will go over how to create a VMware Images for use within VM Essentials.

NOTE

A VM Essentials appliance may have many vCenter Clouds tied to any number of vCenter appliances. If the same images need to be available to multiple vCenter Clouds, you will need to download the OVF from one vCenter and upload it into the others. At that point you can make multiple VM Essentials Node Types from the images and it will be available to all needed vCenter Clouds. This is a vCenter limitation but one which may not be obvious when provisioning via VM Essentials.

Creating a CentOS/RHEL 7 Image

About this task

Create a new virtual machine in VMware vCenter and install a base version of your preferred Linux distro build. If you are using cloud init as part of your image you will need to ensure your virtual machine has a cdrom.

Procedure

1. Before installing the operating system setup a single `ext` or `xfs` partition without a swap disk (This is so that growpart can extend the disk. growpart currently does not support lvm)
2. Install the distro and apply any updates to the operating system and security updates
3. Install cloud-init using command `yum install cloud-init`
4. Install cloud-utils-growpart using command `yum install cloud-utils-growpart`
5. Install open-vm-tools using command `yum install open-vm-tools`
6. Install git by running `yum install git`

7. Install epel-release repo using command `yum install epel-release`
8. selinux set to permissive (enforced can cause problems with cloud-init) `sudo vi /etc/selinux/config`

Subtopics

Cloud-Init
Network Interfaces

Cloud-Init

To get started with a base CentOS image we first install cloud-init. This is a relatively simple process using yum:

```
yum -y install epel-release
yum -y install git wget ntp curl cloud-init dracut-modules-growroot
rpm -qa kernel | sed 's/^kernel-//'  | xargs -I {} dracut -f /boot/initramfs-{}.img {}
```

There are two parts to this yum installation. We are first ensuring some core dependencies are installed for automation as well as cloud-init. git for example is installed for use by ansible playbook automation down the line and is therefore optional if not using ansible. The dracut-modules-growroot is responsible for resizing the root partition upon first boot to match the virtual disk size that was potentially adjusted during provisioning.

A great benefit to using cloud-init is credentials don't have to be locked into the blueprint. It is advisable, within VM Essentials , to configure the default cloud-init user that gets created when the vm boots automatically by cloud-init. This is located in Administration > Settings > Provisioning, within the Cloud-Init Settings section.

Network Interfaces

A slightly annoying change with centOS 7 is that the network interfaces have changed naming convention. You may notice when running ifconfig that the primary network interface is set to something like ens2344 or some other random number. This naming is dynamic typically by hardware id and we don't want this to fluctuate when provisioning the blueprint in various VMware environments. Fortunately, there is a way to turn this functionality off and restore the interface back to eth0.

Firstly we need to adjust our bootloader to disable interface naming like this.

```
sed -i -e 's/quiet/quiet net.ifnames=0 biosdevname=0/' /etc/default/grub
grub2-mkconfig -o /boot/grub2/grub.cfg
```

The above command adds a few arguments to the kernel args list (namely `net.ifnames=0` and `biosdevname=0`. It may be useful to view the `/etc/default/grub` file and ensure these settings were indeed applied.

The next step is to adjust the network-scripts in centOS. we need to ensure we have a file called `/etc/sysconfig/network-scripts/ifcfg-eth0`

Below is a script that we run on our packer builds to prepare the machines network configuration files.

```
export iface_file=$(basename "$(find /etc/sysconfig/network-scripts/ -name 'ifcfg*' -
not -name 'ifcfg-lo' | head -n 1)")
export iface_name=${iface_file:6}
echo $iface_file
echo $iface_name
sudo mv /etc/sysconfig/network-scripts/$iface_file /etc/sysconfig/network-
scripts/ifcfg-eth0
sudo sed -i -e "s/$iface_name/eth0/" /etc/sysconfig/network-scripts/ifcfg-eth0
sudo bash -c 'echo NM_CONTROLLED=\"no\" >> /etc/sysconfig/network-scripts/ifcfg-
eth0'
```

This script tries to ensure there is a new ifcfg-eth0 config created to replace the old ens config file. Please do verify this config exists after running. If it does not you will have to be sure to build one on your own.

```
TYPE=Ethernet
DEVICE=eth0
NAME=eth0
ONBOOT=yes
NM_CONTROLLED="no"
BOOTPROTO="dhcp"
DEFROUTE=yes
```

Creating a CentOS/RHEL 8 Image

Create a new virtual machine in VMware vCenter and install a base version of your preferred Linux build. You must be running ESXi 6.7 Update 2 or later.

Subtopics

- Prepare The New CentOS 8/RHEL8 Image
- SELinux Settings
- Network Interfaces
- Final VMWare Tasks
- Creating an Ubuntu 20.04 Image

Prepare The New CentOS 8/RHEL8 Image

Procedure

1. Install epel-release: `yum -y install epel-release` (This step is not necessary for RHEL)
2. Install git, wget, curl, cloud-init, cloud-utils-gropart, and open-vm-tools: `yum -y install git wget curl cloud-init cloud-utils-growpart open-vm-tools`
3. Update: `yum -y update`
4. Finally run: `rpm -qa kernel | sed 's/^kernel-//' | xargs -I {} dracut -f /boot/initramfs-{}.img {}`

SELinux Settings

About this task

If allowed by your internal IT policies, set SELinux to permissive to avoid potential issues with cloud-init down the road.

Procedure

1. Edit the following: `vi /etc/selinux/config`
2. Make the following change: `setenforce 0`

Network Interfaces

About this task

Run the following to rename the network NIC. Values inside angle brackets should be filled in with the appropriate value for your environment (ex. <varname>):

Procedure

1. `sed -i -e 's/quiet/quiet net.ifnames=0 biosdevname=0/' /etc/default/grub`
2. `grub2-mkconfig -o /boot/grub2/grub.cfg` (location may be different, could be located at /boot/efi/EFI/centos/grub.cfg)
3. `ifdown <orginal-nic>`
4. `mv /etc/sysconfig/network-scripts/<orginal-nic> /etc/sysconfig/network-scripts/ifcfg-eth0` (this changes name/device to eth0)
5. Edit `ifcfg-eth0` and change the NAME to `eth0`
6. `bash -c 'echo NM_CONTROLLED=\"no\" >> /etc/sysconfig/network-scripts/ifcfg-eth0'`
7. `ip link set <orginal-nic> down`
8. `ip link set <orginal-nic> name eth0`
9. `ip link set eth0 up`
10. `ifup eth0`

Final VMWare Tasks

Procedure

1. Detach any install media
2. Shutdown the VM
3. Convert the VM to template on the VM Essentials side
4. Refresh the VM Essentials Cloud to allow the new template to sync

Creating an Ubuntu 20.04 Image

Download the Ubuntu 20.04 ISO from Canonical, and upload the base image to vCetner. Then, create a new virtual machine in vCenter.

NOTE

Since we'll include cloud-init with our image, we will need to ensure the virtual machine has a cdrom. Select the Ubuntu 20.04 ISO we just downloaded from the CD/DVD drive dropdown menu when creating the new virtual machine.

Before installing the operating system, set up a single ext partition without a swap disk. Then, continue on installing Ubuntu making the following selections during the setup process:

- Update to the latest installer if a later version is available
- Use the entire disk and deselect the option to set up the disk as an LVM group
- Configure an account and set a password
- Opt to install OpenSSH Server

- Other optional packages aren't needed for this basic Ubuntu image

Complete the installation process and reboot the machine. Update the package list and apply any upgrades:

```
apt-get update
apt-get upgrade
```

Change the network interface to `eth0` by editing `/etc/default/grub`. The line `GRUB_CMDLINE_LINUX=""` should be edited to `GRUB_CMDLINE_LINUX="net.ifnames=0 biosdevname=0"`.

Update GRUB:

```
update-grub
```

Update the `70-persistent-net.rules` file:

```
cat << EOF > /etc/udev/rules.d/70-persistent-net.rules
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{dev_id}=="0x0",
ATTR{type}=="1", NAME="eth0"
EOF
```

Remove `subiquity-disable-cloudinit-networking.cfg` as cloud-init will skip network configuration if it's present:

```
rm -f /etc/cloud/cloud.cfg.d/subiquity-disable-cloudinit-networking.cfg
```

Update `99-pve.cfg`:

```
cat << EOF > /etc/cloud/cloud.cfg.d/99-pve.cfg
datasource_list: [ConfigDrive, NoCloud]
EOF
```

Remove Netplan files, they will not be regenerated if they exist:

```
rm -f /etc/netplan/00-installer-config.yaml
rm -f /etc/netplan/50-cloud-init.yaml
```

Run cloud-init clean:

```
cloud-init clean
```

Next, reboot the system and confirm the network interface is labeled `eth0` once the machine comes back up. Then, clear BASH history for root. The history entry has a copy in the memory and it will flush back to the file when you log out. You can avoid this with the following command:

```
cat /dev/null > ~/.bash_history && history -c && exit
```

Shutdown the system:

```
shutdown -h now
```

Convert the VM to a template in vCenter before moving back to VM Essentials to onboard the image and use it to begin building your provisioning library.